BIRD Proposal

KAZUAR Advanced Technologies Ltd. - Patriot Technologies Inc.

06.04.17

Israel-U.S. Binational Industrial Research and Development Foundation

From: Israeli Company**: KAZUAR Advanced Technologies Ltd.**

Office Address -
154 M.Begin Rd., Kardan Bldg.
Tel-Aviv, Zip code 6492107, Israel
Telephone No. +972 (50) 7799000
Fax No. +972 (3) 3721112

Mailing Address -
154 M.Begin Rd., Kardan Bldg.
Tel-Aviv, Zip code 6492107, Israel

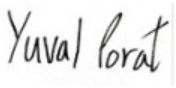
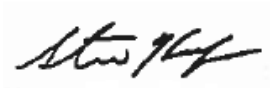
From: U.S. Company: **Patriot Technologies Inc.**

Office Address -
5108 Pegasus Court
Frederick, MD 21704
Telephone No. +1(301) 6957500
Fax No. 301 695 4711

Mailing Address -
Patriot Technologies Inc.
5108 Pegasus Court Frederick, Maryland 21704

Project Title: Intelligence-grade security comprehensive solution designed for non-IT experts

Project Duration: 24 months **Project Budget: $3,125,816** (1)

Submitted by:	**Israeli Company Authorized Company Official**	**U.S. Company Authorized Company Official**
Signature:		
Printed Name:	Yuval Porat	Steve Keefe
Title:	CEO	President & CEO
E-mail:	yuval@kazuar-tech.com	steve@patriot-tech.com
Date Submitted:	April 6ft,2017	April 6ft,2017

(1) Project Budget – must be the same as the sum of the companies' budgets

Preferred date (month / year) for start of project funding (2) 01/08/2017

(2) Do not request a start date prior to the date of the final proposal submission.

B. Table of Contents

C. Executive Summary of BIRD Project Proposal

	Israeli Company	U.S. Company
Company name	KAZUAR Advanced Technologies Ltd.	Patriot Technologies Inc.
Company locations (headquarters and relevant division address, including full street address, state, city, zip code)	154 M.Begin Rd. Kardan Bldg., Tel-Aviv, Zip code 6492107, Israel	5108 Pegasus Court Frederick, MD 21704
Company website	www.kazuar.info	www.patriot-tech.com www.patriotcyber.com
Year established	2014	1996
Revenues: most recent fiscal year 2016	$188 K	$32.5 M
Increase / (Decrease) over previous year	812%	22%
Number of employees	8	35
Ownership (Public / Private)	Private	Private
Percentage ownership of the company by the other company	-	-
Relationship of the companies – - Parent/Subsidiary - Common Ownership - No common relationship - Other	No Common relationship	
Number of previous BIRD projects	-	1 in 2014

C1. Abstract

This project is a collaboration between KAZUAR - an Israeli start-up and Patriot - a well-established US company. KAZUAR - a pioneer in developing a comprehensive secure work environment founded by leading security experts, and Patriot - a provider of secure, tailored solutions to global government and commercial customers. Together, they will develop an innovative comprehensive end-to-end solution, which makes intelligence-grade security accessible to businesses, and allows them to work conveniently and securely from anywhere. To reach this unprecedented security level, a self-contained, hardware-encrypted work environment will be created and will be accessible only to its users. The system will be developed as a whole, and will include the development of a unique PC device, and various options for secure i/o devices, such as encryption based keyboard, mouse and screen. The device will enable access to a highly secure private cloud. The system will also provide its users with an innovative technology based privacy and complete control of their data by providing them with zero-trust infrastructure and sole ownership and governance over their private encryption keys. The solution is designed for non-IT experts and provides exceptional user-experience. The project budget is expected to be split, with 70% allocated to KAZUAR and 30% to Patriot. A full solution ready for sales is expected by the project's end. The market of cloud security is extensively growing, expected to reach more than $4B by 2022. The total accumulative sales are expected to be $55M (2020 – 2022).

C2. Company Background

KAZUAR Advanced Technologies Ltd. (KAZUAR), headquartered in Israel, develops innovative solutions for customers who require the highest level of security. The company has developed holistic cyber security solutions based on extensive experience in intelligence, cyber-security and strategy. KAZUAR's flagship solution is a secure PC environment, which includes KAZUAR secure PC and the “Fortress”. KAZUAR secure PC is a tamper-proof security device which self-destructs upon any attempt to hack it, and meets the highest standards of the United States Department of Defense. It connects to any computer, transforming it into a Secure PC. The heart of the system is KAZUAR’s Fortress, which is a secure private cloud located in a highly confidential physical location and has a unique design. The fortress is protected by multi-layer, state-of-the-art technologies and security strategies.

The system has a proven track record of thwarting massive state coordinated cyber-attacks. Once connected to the Fortress, users enjoy an end-to-end, encrypted and isolated workspace. Information cannot be sent out of the Fortress unauthorized or unnoticed, thus preventing internal leaks. KAZUAR's solutions are user-friendly as they allow secure access to the Fortress from any computer, using the familiar Windows software applications used by the customer. KAZUAR's solution easily integrates with the customer's existing work environment. Even though KAZUAR is a relatively young company, it has already begun to make sales and generate revenue. Additionally, KAZUAR is one of the 10 Israeli companies that were chosen by Intel to participate in Intel Ingenuity Partner Program (Intel IPP). **Yuval Porat**, co-founder and CEO, has 20 years of experience and proven record in strategy design, crisis management and branding. **Moshe Azar**, co-founder and CTO, has extensive experience and a proven record in data security, telecommunications and business management. For 20 years, he owns and manages a leading, highly successful IT company that designs and implements solutions for various complicated and sensitive mission critical projects around the world. **Shimon Erlichman**, who serves at the board of advisors, was the CTO and the deputy director of one of Israel's key government security organizations. He brings great technological depth and breadth of knowledge across numerous fields of science and technology.

Patriot Technologies, Inc. (Patriot), headquartered in Frederick, MD, is the trusted advisor that provides secure, tailored hardware and software solutions to global government and commercial organizations based on a thorough understanding of their business environment, market developments, and organizational goals.
For over 20 years, Patriot delivers solutions that leverage and go beyond industry standard products, and addresses all aspects of a technology development life-cycle – from consulting and designing a solution, to integrating, implementing, and managing the ultimate deliverable. Patriot has a proven track record of success with hardware and software solutions with an emphasis on security. Patriot has a variety of expertise in the fields of cyber-security, infrastructure protection and control systems monitoring, mobile and network security and specialized hardware and software solutions, manufacturing and logistics services and product sourcing. In addition, Patriot has a cleared facility for Secure Supply Chain requirements. They have over 60 active customers including government agencies, Fortune 1000 clients, IT security software vendors, DoD system integrators, communications equipment vendors, and communications equipment service providers including Raytheon, IBM, Check Point, United States Air Force Auxiliary Civil Air Patrol, NAVFAC, Frontier Communications and McAfee. **Steve Keefe**, President & CEO, has over 30 years of management and technical experience in the software development and manufacturing sectors. Prior to Patriot, he spent 8 years working on projects with NSA with emphasis on real time operating systems and data acquisition. He also spent over 10 years working on a variety of technical engineering activities related to hardware, software, firmware and application in use by large and small companies. **Dewayne Adams**, CTO, is responsible for engineering, integration design, information technology and marketing. He has extensive experience in solution development and successful deployment. He created first zero client laptop, first switchable multi-domain remote desktop, advances in wearable computers and 3 patents covering these innovations along with other at NYNEX Science & Technology, Xybernaut and NCS Technologies. He also holds a Top Secret security clearance.

C3. The Innovation

The solution is a dedicated, end-to-end secure computing stack including secure hardware, firmware, operating system, peripherals, software suite, communications and services, in order to create a highly secure yet highly productive work environment for high-profile organizations. The innovation lies in its holistic approach to security, firmware & software design, zero-trust infrastructures, hardware design, unprecedented level of security, and user experience.

Holistic approach to security
Commercial security products today take a direct approach to solve a specific problem such as Antivirus, firewall, IDS or IPS, leaving other problems to be addressed by other vendors. This leaves customers with unavoidable vulnerabilities, seeking different products and a way to properly integrate them together and into the organizational workflow. The developed solution is based on a different innovative approach to offer a comprehensive solution. It will provide the customer with ever maintained secure, private and trusted environment looking at work processes, threat vectors and models of high-profile targets and designing an approach which considers the system as a whole: hardware, software, user, organization and workflows.
The solution will consider how each part influences the others, how it hinders security and how it can be secured and promote the security of other components. The solution will be designed to ensure the all components together provide unparalleled security and privacy.

Software Design
The solution introduces a truly “red” secure work environment, which is cryptographically isolated from any threat residing on the operating system. The software methodology is encryption based CPU extensions, also taking into account that each of the user's activities (surfing the web, writing a document etc.) is reflected by at least one end device, e.g. a keyboard, a mouse and a screen. Therefore, the R&D approach will focus on encrypting the input and output of these devices (typing, mouse movements etc.). In order to maximize the security level and to create a secure and trusted software suite, the encryption process will utilize Intel’s new secure CPU feature – SGX. An SGX cryptographic library will be developed, aiming to create significantly lower resource usage and future-proofing (per same no. of bits of security) which are crucial factors for lower latency and growing threats of rapid increase in computational power. The R&D challenging plan will be built gradually, eventually addressing cloud privacy. This entire innovative approach will allow the user to maintain secure work, even on a compromised environment.

Zero-Trust Infrastructures
The solution integrates zero-trust cloud infrastructure, which will enable customers to maintain the highest degree of technology-based privacy. The customer will have complete control, oversight and governance over their data by being the sole entity controlling encryption keys and other security semantics, and will be protected even from malicious and sophisticated attacks against cloud-based infrastructure (e.g. Hypervisor compromises).

Hardware Design
The solution applies a holistic approach to hardware security. Each component will be designed to be secure independently, while leveraging a cryptographically sound trust between all peripheral to ensure the integrity and security of the system as a whole. The hardware will be designed to be tamper-proof and meet the highest FIPS 140-2 levels of security. As part of it, the R&D will address different outcomes and potential threats to prevent forensics and other data capture techniques, these will include physical tampering measures, destructive, cryptographically signed firmware and electronic destructive safeguards, hence, preventing unauthorized access to the data even in case of physical access by an adversary.

Unprecedented Level of Security
Commercial security products are usually designed to tackle standard threat levels. Due to the shift in the level of sophistication of current threats and KAZUAR's experience in state-backed offensive technologies and operations, the solution will be designed to be the first commercial solution that has the capability to deal with targeted and highly sophisticated threats, including state-backed attacks.

User Experience
The solution does not require comprises to be made between security and productivity, a compromise that users and organizations are often forced to do. Both are equally important

and the solution offers an unprecedented level of security while maintaining the highest level of productivity, ease of use and user experience the end user requires.

C4. Collaborative Relationship

KAZUAR will be responsible for the development of the secure software (multi-layer security, encryption abilities etc.), define the technological features of the hardware components and perform prototypes system tests. Patriot will be responsible for manufacturing the hardware prototypes and performing a series of lab tests (e.g. pen testing and physical tampering), for the development of the hardware manufacturing process and will advise on aspects of US regulation. The hardware detailed design will be jointly developed by both companies. The budget is expected to be split, with 70% allocated to KAZUAR and 30% to Patriot. The non-BIRD portion of the project expenses will be covered by KAZUAR.

The companies agreed that KAZUAR will hold any foreground IP of the developed technology, regardless of inventorship, and will receive all revenues. Patriot will sell the hardware devices that it manufactures to KAZUAR. Patriot will also commercialize the solution in the US as a non-exclusive distributer by using its well established sales and marketing infrastructure.

C5. Commercial Potential

The outcome of this BIRD project is an intelligence-grade security solution designed for non-IT experts. Therefore, its potential market will be composed of organizations holding sensitive and valuable information: (1) Business organizations or specific department within the organization that manage confidential data such as financial bodies, insurance companies, medical manufacturers etc. (2) HNWI – individuals, owners of sensitive information or expensive properties. (3) Government organization such as intelligence, security, international communication etc. As the volume of information held by organizations today is increasing, information becomes more valuable and sensitive. Attackers on the other hand are becoming more complex and sophisticated, and organizations are forced to confront governmental-level cyber-attacks. As a result, organizations these days seek high-end reliable security solutions. Moreover, since the developed solution will be designed to be user-friendly for non-IT experts, it will be fit even for small organizations with no IT departments that require high-end security for their data.

The developed solution will be implemented in two constellations: (1) a premium security system which answers the highest and tightest security requirements for high-end clients (2) a system which provides part of the security abilities at a lower price. This enables the companies to offer a flexible solution that will be suitable for more client's needs and expand the market reach.

The global cloud security market size was valued at USD 282 million in 2014. The market is expected to grow in the coming years due to a variety of factors such as the growing adoption of cloud computing by small and medium enterprises, increasing numbers of smartphones and internet users, and the growing concern of the safety of information and data over the cloud. The market is expected to grow at an annual growth rate of 42%, exceeding $4 billion in annual expenditures by 2022.

The solution's business model is comprised of an initial set-up fee and fees for ongoing secure-cloud services.

Calendar year	**2020**		**2021**		**2022**	
The Solution Type	**Lite**	**Premium**	**Lite**	**Premium**	**Lite**	**Premium**
Target market size for developed product (M$)	2,312		3,283		4,662	
Estimated market share (%)	-		0.3%		0.8%	
Estimated sales quantity (units)	143	493	1,228	894	3955	2,509
Estimated representative unit price ($/unit) one-time fee	3,000	3,000	3,000	3,000	3,000	3,000
Estimated representative unit price ($/unit) Recurring Service per mount	250	500	250	500	250	500
Estimated sales revenue (K$) one-time fee	430	448	3,617	2,640	11,434	7,079
Estimated sales revenue (K$) Recurring service	218	429	11,896	3,138	9,649	13,246
Total Estimated sales revenue (K$)	1,525		11,291		41,409	
Total Estimated cumulative sales revenue (K$)	1,525		13,286		54,695	

D. The Innovation

List of abbreviations and terms

AMT	Active Management Technology
AV	Antivirus software
CSME	Converged Security and Management Engine, Intel's state of the art firmware control, powering the AMT
DAL	Dynamic Application Loader
ECC	Elliptic Curves Cryptography
Enclaves (secure enclaves)	A secure segment of the SGX code, encrypted and protected from the outside by the CPU [assumed safe from all known intrusions and hacks if used properly]
HDCP	High-Bandwidth Digital Content Protection
HID	Human Interface Device, with reference to a myriad of computer interfacing devices and systems
HSM	Hardware Security Module
Hypervisor	Computer software that creates and runs virtual machines
IDS/IPS	Intrusion detection/prevention systems
Pen-testing	Penetration testing, referring to teams of experts that try to find cyber-breaches in a secure system, for the sake of benchmarking and improving it
RDP	Remote Desktop Protocol, also in a more general term the software that handles the remote desktop client or server
'Red'/'Black' environment	In reference to a system with an encrypted side (that can be transmitted publicly) 'black' and a decrypted sensitive information side 'red'
SGX	Software Guard Extensions
Soc/Noc	Security operation Center/ Network operation Center
TEMPEST	Electromagnetic emissions security, in reference to potential leakage of sensitive information through it
TTP	Trusted Third Party, with regards to encryption keys generation

D1. Background

- **Cyber security is a growing necessity in modern organizations, in face of an increasingly sophisticated threat, and the heightened importance of businesses' data.**
- **Current solutions tend to act separately against specific threats and do not even try to provide holistic protection.**
- **The empirical result is an increasing number of occasions in which critical data is being compromised.**

Data leaks are among the greatest risks to modern businesses, but no defense has been proven effective against sophisticated, 21st-century threats. Existing security products are commonly offered to organizations as separate, multiple black-boxes that usually aim at protecting conventional IT systems. Experience shows that tailored solutions for specific threats have repeatedly failed, and the last several years have shown that even such leading organizations as Sony, J.P. Morgan and Lockheed Martin are prone to attacks and can be significantly harmed by them.

Cloud computing has become a prevalent delivery model for many business applications, therefore being incorporated into the strategy of nearly all leading enterprise software companies. Nevertheless, companies are highly concerned about the introduction of risks to their organizations by the transfer of sensitive data such as customer information, employee data or intellectual property, to the cloud.

Among the relevant scenarios for information and security being put at risk in a seemingly safe environment are "chained compromises" events, in which seemingly unrelated components are being used to breach a full system. A relatively intuitive and highly common example is the usage of a system's boot loader or volume boot record to work-around an existing legitimate OS and reach complete avoidance of anti-virus software.

We are witnessing two parallel trends in the cyber-security world: Data and information are becoming both more voluminous as well as more valuable and the significance of keeping them secure rises in response. Numerous companies seek to protect themselves against industrial espionage. Simultaneously, attacker capabilities are developing and shifting towards higher sophistication, including due to proliferation of state actors' tools and the leakage of capabilities to the private market. Even further, there is accumulated evidence of state actors' active involvement in industrial espionage, and naturally former members of such organizations proliferate the relevant methods and disciplines to the civilian world. The combination of the higher value of attacking and the higher availability of sophisticated tools leave a vast majority of entities unprotected against the relevant threats.

The assimilation of the evolving reality among executives triggers the intuitive instinct of increasing investments in preventative measures. However, accumulated experience shows the extent to which traditional security fails to live up to what it promises.

D2. The Field's Current State-of-the-Art

- **State of the art layered solutions include AV software for conventional attacks, Firewalls, IDSs for reduced accessibility and cloud solutions for monitoring and handling of data storage and transfer.**
- **Significant segments of threats are therefore neglected such as Human Interface Devices (HID)-based attacks, mal-intending physical visitors and escalating low-level hardware attacks.**
- **The customers' need to integrate multiple technologies and solutions entails additional costs, complexity and effectively reduces security.**

Hardware

In a standard working environment, every piece of interfacing technology can serve as an attack surface. For the sake of understanding the hardware-based threats and current solutions, we examine several examples of non-trivial hardware attack methods that are de-facto compromising multiple operational systems:

1. The End Point Computer Itself

Computers today are blindly trusting any HID. This allows for highly-sophisticated physical attacks in the form of HID impersonation for code injection. Gaining physical access to a computer is often a "game-over" scenario, enabling a skilled attacker to leverage said physical access into a widespread access to multiple parts of the system, and extract valuable data. Even when disk encryption is employed, sophisticated attackers often have means to extract data from residual memory modules, NAND devices and similar hardware components. Moreover, fundamental design concepts in modern operating systems (e.g. automatically activate and honor network device attached to a running computer) can be (and actually are) being exploited to gain full control of the system regardless of security mechanisms.

2. Keyboard

Keylogging (the process of maliciously recording keyboard keystrokes) can be carried out by an advanced attacker using a wide range of tactics. Physical tampering of a keyboard is extremely challenging to detect yet easy to conduct, and similarly, physical keyloggers with remote access are simple to install covertly. When carefully implemented, software keyloggers can be deployed on a machine without triggering any security prevention measures due to the nature of the involved Syscalls (the OS system calls). In these cases, software mitigation tools (such as antivirus softwares) are limited in their effectiveness. Wireless peripheral devices are even easier to intercept.

3. Display

Displays and display-like devices (e.g.: HDMI Recorders) can serve as attack vectors enabling screen grabbing or content recording, while current solutions to mitigate this threat (namely HDCP) have been long breached.

Moreover, malware extensively using screen grabbing techniques in order to capture application outputs for various phases of attack (either recon for lateral movement, privileges escalation, internal system exploitation, data exfiltration and so forth). These malware ranges from simple bitmap buffer scraping to sophisticated driver-level memory

grabbing. Once such malware exists on a computer (evading the installed mitigation software) there's very little that an organization can do in order to prevent this form of data disclosure).

Most existing products that aim to prevent security compromises function on the OS level (AVs, human-IDS, antimalware, whitelisting etc.), or on the network level (network-IDS/IPS, firewalls). Very little effort has been put into securing the actual hardware that has led to hardware-originated compromises in recent years. Highly motivated adversaries will use the lack of security of hardware peripherals and other physical components in order to access a secure system. In many such cases, we find hardware based wireless key loggers, pre-installed non-secure operating systems, pre-infected storage devices and other creative attacks.

While few attempts to create secure peripherals have been made in the past, they all failed in one way or the other: Encrypted wireless keyboards can be easily circumvented with software key loggers on the OS. Hardware limitations in some products and the improperly integrated cryptographic subsystems led to poorly implemented encryption while hardware that did have sound security didn't offer any better security once the encryption was opened on a compromise host (due to memory scraping attacks).

Software

Most security solutions today take a direct approach to solve a certain problem (Anti-virus, firewall, IDS or IPS) leaving other problems to other vendors. This leaves the end user and end organization ever chasing for different solutions and even worse, seeking for a way to properly integrate all said solutions together as a system and into the organizational workflow.

In modern solutions, once a system has been compromised, there is very little (if anything) that a user can do to protect sensitive data and to prevent further escalation such as compromising encryption keys. Attacks such as memory scraping and process injection can be easily carried out once an attacker gained basic access.
In addition, even the most widespread solutions for secure IT, often present the users with a tradeoff between security level and productivity. It is not uncommon to find disgruntled employees due to the restrictions and inconvenience that security systems pose on them. This tends to become more evident as organizations are larger, and potential attackers are more capable on the one hand, while the systems are more complex and harder to defend.

Further to current state of the art security and convenience, only very few cloud solution vendors offer true zero-knowledge products. In a zero-trust environment, encryption keys (complete or partial) should be completely unknown to the vendor providing the cloud services, in addition, these keys should not be limited to file storage or emails. With most cloud providers, and definitely with the ones that provide virtual computing, the client is forced to blindly trust the vendor and the hypervisor.

Trusting the hypervisor is a critical security drawback: A virtualized operating system running in a cloud provider, along with all of its memory space, running processes, manipulating and storing data, etc., is completely transparent to the Hypervisor. A malicious employee working for the provider, a subpoena served to the provider by a state or state-representing entity, a compromise at the hypervisor level or cross VMs compromises, all puts the clients VM (and

data) at great risk.

Since this problem is so severe and with no practical answer, it had two unfortunate outcomes:

a. It forced users of cloud-backed services to willingly disregard the problem and put their fate in the good will of the provider.
b. It literally prevented the adoption of cloud-backed solution at huge market sectors (namely, sensitive government agencies or security-conscious enterprises)

Security capabilities of existing solutions today:

We can compare the current capabilities of some leading solutions in the cyber-security field. This comparison is obviously not a full one, but serves to show how partial solutions are lacking at least in some fields, and naturally combined solutions require integration and extended expenditure.

The right column presents KAZUAR's first generation product as one of the compared technologies. This solution offers a secure bootable device which enables users to boot any computer into a secure, trusted operating system. While the first-generation solution is a successful operational product with a proven record in eliminating state-sponsored breaches, throughout the use of the product, the need for a device with a much wider and deeper approach was noticeable. Nevertheless, as can be seen in the chart, the first generation is a much better solution than any other available security product, providing protection from most known attack types. However, it still does not provide a comprehensive solution to every known attack vector.

Prevention of common attack types - high level threat types from an operational point of view:

	IT Solutions	Bromium	Silent Keys	ORWL	Qubes OS	Tails	KAZUAR
Malware / Viruses / Intrusions	○	●	●	○	○	●	●
Outsider Attack	◐	○	●	○	○	●	●
User Error	●	○	○	○	○	○	●
Service Provider Failure	●	○	○	○	○	○	●
Physical Security (e.g. loss/theft of equipment)	○	○	◐	●	○	●	●
Misuse of mobile device / OS Vulnerability	○	●	○	○	○	○	●
Insider Sabotage	○	○	○	○	○	○	●
Cloud apps for service usage	○	●	○	○	●	○	●
Partners	●	○	○	○	○	○	●
Data Explosion or data-related vulnerability	●	●	○	○	●	●	●
Activist groups	○	●	●	●	○	○	●
Phishing	●	○	○	○	○	●	●

Protection against specific attack vectors - technological description of major attack types

	IT Solutions	Bromium	Silent Keys	ORWL	Qubes OS	Tails	KAZUAR
Physical tampering - FIPS 140-2	○	○	○	"Striving to get certified"	○	○	●
Unidentified Trojan at the endpoint	○	●	○	○	●	○	●
Hacking communications (Man in the Middle, stealing keys)	○	○	●	○	○	●	●
Attacking the OS	◐	●	○	○	●	○	●
Attacking BIOS	◐	○	○	●	○	○	●
Trojan on the server	○	○	◐	○	○	○	◐
Physical attack on the keyboard (such as physical keyboard sniffer)	○	○	◐	○	○	○	◐
Replacing the keyboard	○	○	○	○	○	○	○
Physical attack on the screen	○	○	○	○	○	○	○
Replacing the screen	○	○	○	○	○	○	○

Protection against specific attack vectors - technological description of major attack types

	IT Solutions	Bromium	Silent Keys	ORWL	Qubes OS	Tails	KAZUAR
Screen sniffing	○	○	○	○	○	○	◐
keylogger	○	○	○	○	○	○	◐
Identity theft	○	○	○	○	○	○	●
Stealing files by a user ("Snowden scenario")	○	○	○	○	○	○	●
Accessing unpermitted files ("Snowden scenario")	○	○	○	○	○	○	●
Protection against malicious user trying to steal credentials	○	○	○	○	○	○	●
Replacing the screen driver	○	○	○	○	○	○	◐
Internal attack by admin / cloud provider	○	○	○	○	○	○	◐

Usability - system capabilities from the functional user's point of view

	IT Solutions	Bromium	Silent Keys	ORWL	Qubes OS	Tails	KAZUAR
Immediate implementation	○	○	●	●	○	●	●
Simplicity, not IT expertise needed	○	○	●	●	○	○	●
Provided as a service	○	●	○	○	●	○	●
Server side solution	●	○	○	○	○	○	●
Mobility	○	○	◐	○	○	○	●
Provides an organizational solution for businesses	●	●	○	○	○	○	●
Provides a comprehensive plug & play solution	○	○	○	○	○	○	●

In this comparison, one can observe the point of failure of the current leading approaches. Any type of sophisticated attack or a combined one is likely to put a vast majority of highly protected systems at risk. This is a direct result of vendors neglecting the scenario of state-funded attacks or, as becomes more prevalent, an attack inspired by state-funded organizations. These threats become more prevalent and more real as knowledge proliferates, former employees of secret services publish or sell it, and as states become more involved in cyber industrial espionage.

The goal of this BIRD project is to develop an advanced system which provides protection against the widest variety of potential threats and under extreme circumstances, including after a part of it was breached, while maintaining an ideal level of productivity.

D3. The Product's Concept

- **A complete secure system that includes pocket PCs, peripheral user interface, and a connection to a cloud system. All connected together in a manner that prevents attack on them, between them or grabbing information from them.**
- **The provided system is a fully functional user friendly device that enables an organization to replace common computers with a superbly secure solution.**
- **At the foundations of this approach lies significant compartmentalization between components and processes.**
- **Applying additional security measures meeting the highest existing standards and de-facto setting a new standard that meets intelligence grade-security in the civilian world, and includes authentication, foul-play detection, immediate response, and even the ability to work in a compromised environment.**

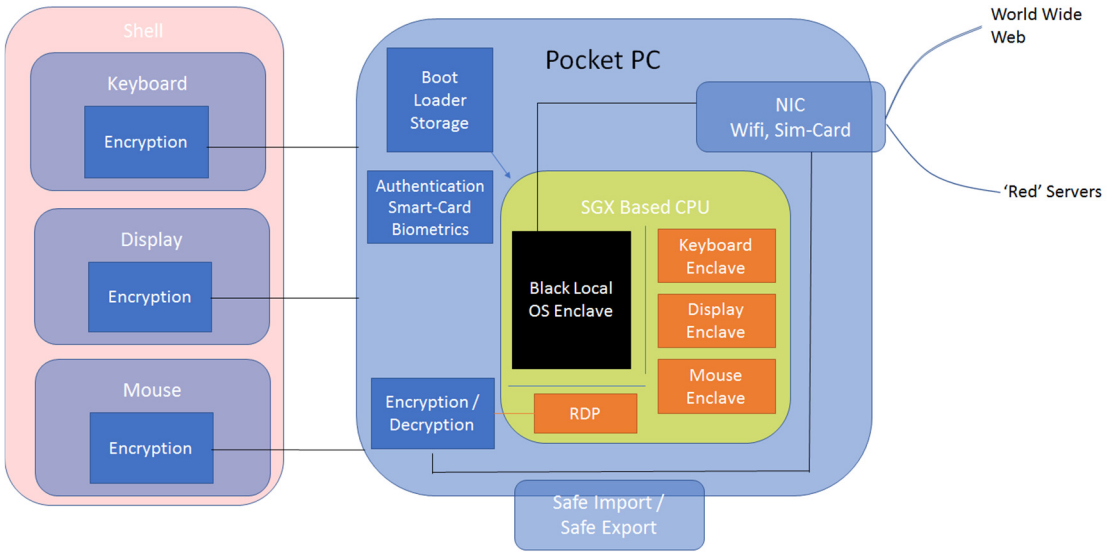
As described above, the current cyber-security market's agenda is that vendors address separate threats with separate solutions. This means that while trying to provide full protection against a specific problem, a supplier would leave other problems neglected. The BIRD project system aims to change this basic perception at its seams.
Furthermore, civilian cyber-security firms set their reference for threats at specific levels that are almost always not the highest one. This means that a vast number of known threats is left unhandled, including combined attacks that leverage physical access into cyber capabilities, highly sophisticated low level attacks that change firmware, the installation of espionage hardware and so forth.

As opposed to existing solutions, the described product is a complete solution that includes end point users' hardware, front end software and back-end cloud infrastructure and software. Supplying a single product that includes all these is a key point in reaching a new level of security, thus providing intelligence-grade security to civilian enterprises and customers. It is required to provide a truly 'red' secure system and complete privacy even from the vendor itself. The basic parts of the system in development, in reference to the block diagram below, are:

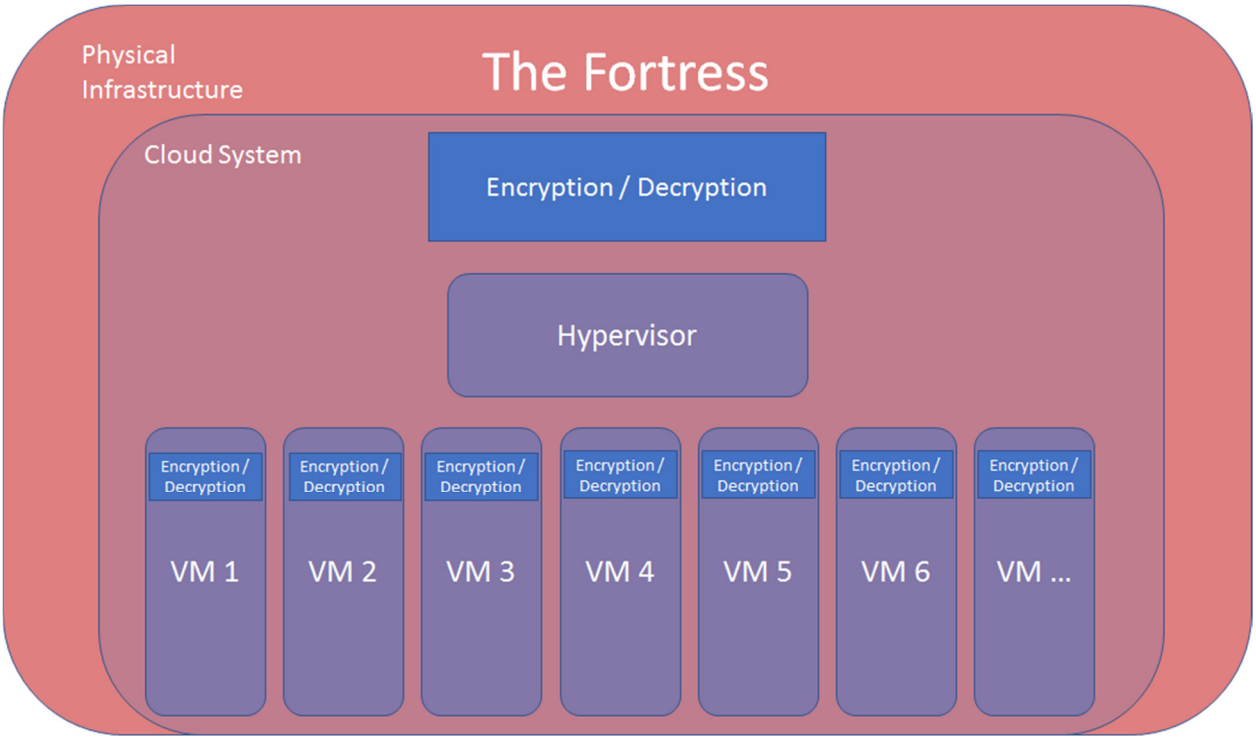
1. A hardened computer hardware - a first version will be based on a pocket-computer, meaning a device that has a motherboard, CPU and connectivity capabilities with potential interfaces to displays and HIDs.
    a. UEFI firmware with optional communication capabilities (for cryptographic validation, remote attestation and potential remote cryptographic data destruction)
    b. A tightly secure bootloader, with additional cryptographically-backed security measures for trusted OS bootstrapping.
    c. A CPU supporting SGX
    d. A cryptographic component for all internal communications
    e. A network interface card with Wi-Fi and cellular based (Sim card) communications
    f. Physical tampering countermeasures
    g. Additional encryption hardware
2. A 'shell' hardware supplying UI -
    a. a hardened display system
    b. a hardened keyboard system
    c. a hardened mouse system
    d. potential additional interfaces

3. A physical server system, based on the Fortress, that runs a cloud system including a hypervisor controlling multiple separate VMs, following SGX programming running separate processes on different secure enclaves.
4. End point's firmware and CPU design to allow a dual environment ('red' and 'black') maintaining functionality and security.
5. Front end software that interfaces with the user and OS.
6. Secure import mechanism
7. Secure export mechanism
   a. Server side export mechanism
   b. End point export mechanism

End-point block diagram:



Server high-level schematics:



The requirements of each of the components separately, as well as from the system as a whole are to prevent any type of security compromise by being mechanically hardened against tampering, logically secure by transmitting only encrypted information between any two components and completely compartmentalized between 'red' storage and software and 'black' information such as internet access. Server-side security is achieved via software and hardware means (AVs, FWs, SGX implementation), as well as physical security of the servers themselves.

All of the system elements are hardened to meet the highest level of security, alongside with using the most up-to-date security technology. This is done by a fully aware design, periodic examination by security experts, red-teams and Pen-testing.

To ensure the customers' trust, all components, concepts and resulting products will be tested and approved by a committee of world-renowned security experts. The cryptographic semantics will strive to be modern, advance and thoroughly validated against recent research in cryptanalysis (e.g. ECC, the next generation of public key cryptography, based on currently understood mathematics, provides a significantly more secure foundation than first-generation public key cryptography systems).

Functional Description

The system is providing the customers with a full computing and data solution that allows mobility and connectivity while maintaining the extreme security requirements stated above. We can follow the basic process of the device's usage.
When the computer device is connected to the 'shell' that holds the UI peripherals, the boot loader is powered and read from a designated storage component in the computer's board and to the CPU.

The user is requested to enter a code to allow the OS to continue its uploading process. After a certain number of entering a wrong code, the device will wipe itself following progressive cool-down periods for failed attempts.

A successful permission grant results in the activation of a local OS on the device's CPU. This OS serves the user as a normal computer while the peripheral devices use the CPU's SGX secure enclaves, thus preventing compromise between the components.

When the user wishes to access the 'red' system that includes sensitive information, he requests access to the Fortress's server. A designated authentication software, implemented on a different enclave will connect to the 'red' server's' environment and request access by using a smart-card device, potential biometrics and an OTP code that will be supplied via a parallel connection such as a phone's designated application (in order to avoid the usage of SMS text messages as recommended by NIST). The servers will validate the user in the two-factor authentication and its status and will grant access accordingly.

Once a connection was established, an RDP session will be opened through the local CPU, and allow working with the peripheral UI on a remote 'red' desktop. All processes are SGX separated and all transmitted data is encrypted between any two components. The usage of SGX and encryption allows hiding and protecting the 'red' system from potential unprotected processes that may run on the CPU in parallel.

All communications that are transmitted to the server systems are encrypted in two layers - the external layer is decrypted by the cloud hypervisor at the entrance to the server, and rerouted to the proper VM while protecting sensitive information from the hypervisor, other VMs and the supplier itself. The second layer of encryption is only decrypted within the sealed VM, where the actual actions are taking place.

Encryption keys are generated by trusted third parties (TTPs) facing the customers themselves to follow the zero-trust requirement and guidelines.

The VM is implemented with SGX processes, meaning different processes on the same hypervisor cannot access unauthorized regions in the memory. This is obviously also true for accessing storage servers via encrypted communications only.

Complementing the functionality, cyber-security and cryptographic solutions, are physical elements that prevent tampering, replacement of components and reading red segments by side-channel attacks. The device will include such solutions as epoxy sealants that prevent physical access to key storage points without their likely destruction, sensors and automatic wiping or locking mechanisms when tampering is detected, using of non-common elements that are more challenging to handle under time constraints. Wiping will comply with the leading standards in the field, and for example the current NIST 800-88 standard.

The described solution applies a holistic approach for hardware and software security. Each of its components will be designed to be secure independently, while leveraging a cryptographically sound trust between all peripheral to ensure the integrity and security of the system as a whole. The hardware will be designed to be tamper-proof and meet the highest

FIPS 140-2 levels of security. As part of it, the R&D will address physical tampering situation by applying destructive cryptographic solutions, cryptographically signed firmware and electronical destructive safeguards, hence, preventing physical access to private information.

Major challenges

Following the system design and the integration of multiple softwares, there are several key aspects that can be recognized as major development challenges:

- Secure Input - Creating a truly secure HID which is cryptographically sealed against keylogging of any type (hardware, software, physical tampering, memory scraping and so forth). The solution lies in the design and implementation of secure protocols that are based on compartmentalization and strong encryption on every point that is susceptible to attack.
- Secure Output - Creating a means of displaying content on screen which is secure against screen grabbing, recording, tampering and so forth. Based significantly on the same means of secure inputs, and requires proper development and testing.
- Safe import and export - creating any type of connection between 'red' systems and 'black' systems is always challenging. Keeping a secure import system uses multiple AV softwares, requires authorization of relevant personnel and monitors and logs the entire process constantly.
- Enabling an end user to maintain work even when the system is clearly compromised.
- Creating a true zero-trust cryptographically secure execution environment for hypervisors, meaning that under no circumstances can a hypervisor (the supplier) willingly access sensitive customers' data. This can be executed with proper encryption logic that separates the sensitive information from peripheral data and allows transmission and handling of encrypted packets within the 'red' server.
- Creating a solution that won't favor security over productivity or vice versa, but will offer the highest level of both. This is a tradeoff that needs to be refined constantly and kept somewhat configurable to meet exact customer's demands.
- Tackle highly critical threats such as an insider threat or physical tampering which are often left unanswered.

Examples of Attack Vectors and Solutions Analysis:

- **An example of the analysis of attack vectors and solution is given.**
- **Many of the vectors have never been dealt with before in the civilian world.**

In order to present a major part of the development process, examples of attack vectors, and the product's solution is provided. It should be noted that the full analysis of numerous attack vectors exists and updates with the ongoing project, but is beyond the scope of this description and can supplied separately:

Attack Scenario	Details
Trojan code running on the computer:	

Attacking the operating system	Using SGX's secure enclaves, meaning that sensitive code and data cannot be accessed, even if the OS is compromised. Potentially, combined with a read-only ghost image OS that can only be updated using a hardware and an SGX updater solution that will receive updates via an AMT connection
Attacking the BIOS	Using Boot Guard makes it nearly impossible to attack/replace the BIOS and install a rootkit at this level. Using a lean BIOS as a development guideline makes it even harder to find breaches.
Malicious user ("Snowden scenario"):	
Exporting files from network	Only authorized users will be able to export files outside the network.
Accessing unpermitted files	The files are stored securely using SGX on both the client and the Fortress's server and encryption keys that are only accessible to the user who created them by using a smartcard (so even if the malicious user has admin access to the storage server, it will not be able to read the files). Additionally, there is a physical separation between the environments of different customers.
Copying the contents of the RDP	The RDP connection will be secured using PAVP+SGX - the data will be encrypted on both ends SGX enclaves, while locally (client side), the data will be sent using PAVP thus preventing any OS level compromise to gain access to the frames
Physical attacks	
Physical tampering with device	Physical tampering to read the secure enclave and its code/data is most likely unfeasible. The device will meet FIPS 140-2 level 3 or 4 requirements. It will be tamper-proof against physical tampering including a self-destruction mechanism in case of such, and will also include a remote destruction mechanism.
Replacing the keyboard	Production of a dedicated secure keyboard which will include a tamper-proof case and tamper-proof smart-card with a unique certificate that will identify the device. Development and production will be executed in collaboration with an appropriate partner.
Misc.:	
Man-in-the-middle attacks (sniffing network communications)	Using SgxSSL to securely communicate between computers and the Fortress's server - cannot be decrypted by any means. In addition, application level protocol (e.g. RDP) will be encrypted using SGX enclave and appropriate certs, so in

	essence, even if the transport layer will get decrypted by an adversary, the application frames are still encrypted.
Brute Force Attack against key components (UEFI/Bootloader/Smartcard etc.)	Protection against brute-force attacks by an electronic bootloader with automatic self-destruction mechanism (that cryptographically destroys the OS/data when too many incorrect login attempts are made)

D4. Uniqueness and Innovation

- **The presented product originated by setting a reference for potential threats that is unprecedented in civilian cyber-security - defending against state-funded espionage services (assumed the most severe threat) and the entire spectrum below it.**
- **Following the high threat reference required a major paradigm shift compared to any existing product. The resulting approach is supplying a fully functional system that includes all components as a single product - hardware, software and cloud services. All hardened and secured to the highest level.**
- **As part of the new approach, the newest technologies and disciplines in security are being employed. Among others, this is the first known system to use the concept of SGX from end to end.**

The product presented in this document is unique in several ways that set it apart from practically any existing solution that is known to us:

1. Setting the highest possible level of reference of threat as a highly motivated and capable state-funded espionage service.
2. A completely new approach that is needed to meet the high reference - Unifying all cyber-security efforts into a single product that includes both hardware, software and cloud defenses and functionalities, as opposed to requiring integration by the customer.
3. Developing innovative software based on the newest available hardware technology that allows for an unprecedented level of security against sophisticated attacks.
4. Following the approach and the technology in use, a design that can be integrated seamlessly into an organization's workflow without harming its productivity or demanding the employees to learn new disciplines. This is done while still allowing for versatility in the solution and tailoring the device for specific customer requirements.
5. In addition to all of the above described unique aspects, the system assumes zero trust between customer and supplier and effectively eliminates the supplier's ability to gain sensitive information.

The product described herein sets its reference threat level at a highly-sophisticated espionage organization. To the best of our knowledge, no other civilian security vendor or supplier aims at this high level. This set point entails handling with practically any known possible attack, including a combination of gaining physical access (e.g. the usage of human assets to perform malicious or deceived actions), physical tampering the includes covert access to devices by a skilled technical person, prior knowledge and reconnaissance, vast resources and more.

This results in a unique approach and system design that includes providing a full set of hardware, software and cloud solutions, supplied as a single system to the customer. This naturally requires the developers to design and integrated a highly complex system. The uniqueness in design includes both a unique implementation of security concepts, alongside with a unique level of customer interface that allows simple assimilation into an organization. The product is using cutting edge technologies such as SGX as a major guideline throughout the full system, from end devices to back-end, unlike any other known system at this time. It is also applying the most up-to-date cryptographic capabilities including the best of breed cryptographic semantics, throughout all communications that are somewhat prone to attacks or sniffing. In parallel to the security supplying environment, a simple and user-friendly

software is being developed with the purpose of keeping the integration of a new technology into an organization as simple and convenient as possible for the end users and for the IT personnel.

Further to the high security, the system aims to protect the customer from the supplier itself. This means that as opposed to current cloud services suppliers, under no circumstances can the operator of the cloud-based system gain access to sensitive information held by the client. This is done by a dual-layered encryption that starts at the end point's hardware and ends at the relevant customer's VM. To the best of our knowledge, no cloud services supplier provides such a level of privacy that arises from both hardware and software encryption.

Given the uniqueness in performance and implementation, this product is a de-facto dominant strategy for many organizations and entities. By using the already acquired knowledge and experience, we can predict meeting the new set of requirements within this project's scope and thus, provide the market with an extremely needed product.

D5. Patent Status

There are no current patent applications relevant to this project by either KAZUAR or Patriot. The team is considering registering patents in the future, while taking into consideration both the advantages and the disadvantage of exposing major methods, techniques and technologies to potential attackers. Leading lawyers and patent experts will accompany the development process in order to make an informed decision. Security experts will be consulted as well given the highly sensitive field, where major players in non-western states are known to disregard the major implications of IP and use published cyber-related patents for their benefit.

D6. Standards and Regulations

- Both US and European leading standards for data security - PCI, HIPAA (US standard for healthcare data security), ISO 27001 (standard for data security), ISO 27799 (standard for healthcare).
- FIPS 140-2 level 3 & 4 - The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2) - a U.S. government computer security standard used to approve cryptographic modules.
- Security review and pen-testing by Intel's engineers and security experts.
- Pen-testing by renowned consulting firms, such as Deloitte - an important step in order to provide services to financial institutions, major corporations, highly regulated organizations and governmental customers.
- Pen-testing by ex-intelligence security experts from offensive operational units, both from the United States and Israel, who will be asked to simulate a state-backed attack, including highly sophisticated attack vectors while using advanced technology and significant resources - a standard that current commercial products are not able to meet.
- The team plans to encourage both leading regulators and insurance companies to set significantly higher standards for data security. In addition to providing better security for customers, which is required due to new threat levels, it will allow the solution to stand out and will encourage other companies to develop products and solutions providing better security.
- Establishing a "privacy and ethics committee" that will review the unique technology and regulations, in order to ensure its customers that it provide the highest possible level of privacy and that their information is not exposed to us – as their provider.
- All encryption-related tasks are based on known, standardized, well documented well tested encryption algorithms and derivatives (Hashing, KDFs, Signing, etc.). All implementations and pre-configured settings are according to industries best practices, known and published research in cryptanalysis and will be verified by 3rd party domain experts.

All of the above together will provide organization with the peace of mind they need in order to focus on their business and will help us build a reputation as a market leader in the high-end security field.

KAZUAR's team is comprised of technological experts with background in governmental security organizations and the industry. The knowledge and experience in the company includes developing complex multidisciplinary systems while meeting the highest standards in the civilian and security worlds. For example, the team includes Shimon Erlichman, who

was the CTO of one of Israel's leading intelligence organizations and brings unique experience in meeting those standards, and Michael Rothman, who oversaw operations and sales at Cisco and brings extensive experience in dealing with major corporations.
The company's current complete solution received both ISO 27001 and 27799, following a thorough examination process of both the design and the workflow processes in the company. Moreover, the company has a lot of experience in working with Pen Testing experts and customers with unique security requirements. It also has extensive experience in designing intelligence-grade security infrastructures and equipment for governmental organizations.

PATRIOT's business model for 21 years supports the development and productizing of elite cyber security products for high end customers ranging from leading security firms to governmental organizations. Patriot build these solutions user ISO 9001:2015 processes and controls. Patriot's team has been involved with the process and successful evaluation and granting of NIAP/Common Criteria and FIPS certifications.

D7. Prior Governmental Obligations

There are no obligations to other government agencies which have supported any part of the innovation development thus far.

E. Proposed R&D Program

E1. Analysis of the Problem

Currently, to the best of our knowledge, no solution fulfills the requirements stated above, namely providing a comprehensive solution that is truly secure, safe and easy to use.

The baseline of this project is the current operational KAZUAR technology which gives customers the ability to securely work with a well defended server and perform storage and computing operations in a safe and mobile manner. The current devices act as an attachment to existing computers, and hence supply only a partial solution to security by the very definition. The development program described herein aims to use the existing features and understanding and create a whole system that is comprised of all hardware and software relevant components and supplies a full solution for superb security.

We expect challenges in both software and hardware development as new technologies are being developed as part of the essence of reaching the high benchmark of the requirements. In general, some of the key development efforts we expect are:

- Secure endpoint hardware
  - Full physical tamper proofing
  - Destructive cryptography application at various levels including destruction of both volume and bootloader keys
- Secure software for the client side
  - Truly secure, end-to-end protected secure “red” environment, including secure input & output, SSL-VPN and RDP. input and output peripherals with HSM-like private key protection, RDP connection, SSL-VPN
- Secure software for the server-side
  - Protected runtime that will enable either safe VMs or containers to execute code with critical data or application segments protected from the Hypervisor / container-manager
- Secure peripherals
  - HID devices should both perform in extremely low latencies but also offer a solid cryptographic communication channel to the running host.
  - Peripheral devices are often based on extremely low powered low resourced micro controller lacking the compute power to perform the required advance mathematics efficiently.
  - Developing a solid crypto library resilient to known attacks on cryptographic subsystem adds even greater challenges due to the nature of these microcontrollers
- SGX Aware cryptographic library
  - SGX in itself doesn’t protect the cryptographic semantics, hence, it is by all means possible to produce a non-secure or poorly-guarded code. This naturally needs to be avoided.

As described below, the development of the system will focus on thirteen major development challenges, presented in a logical order rather than importance or development complication:

1. Physical tamper proof device - computer
2. Physical tamper proof periphery - keyboard and display
3. Encryption Semantics (intricate design and partial implementation of the cryptographic toolchain)
4. Secure firmware (UEFI)
5. Secure Bootloader (UEFI Application)
6. Signed OS
7. Secure output

8. Secure input
9. SGX Based Communication framework
10. Client software
11. Back-end server software - secure storage and execution
12. Connectivity with the 'shell'
13. Import/Export mechanisms

We present the system's components including the major challenges that need to be solved to get to the required final product in terms of hardware and software:

1. Hardware and Firmware

1.1. Physical tamper proof device – computer

The developed device will be packaged in a high security enclosure that prevents physically accessing hardware components. This is done by using designated sealants and mechanical packaging that are hard to remove (effectively requiring special equipment to remove them, and likely allowing detection of the tampering for wiping, or at least causing the attacker to destroy the system while penetrating it), and a sensors suit monitoring foul-play by such heuristics as humidity changes when package is opened, acceleration profiles and others. Any attempt to achieve physical access to the internal parts will delete the cryptographic key, rendering it permanently inaccessible. The device will have a separate sub-system containing a secure microcontroller, this microcontroller utilizes the physical shell and provides continuous physical monitoring and protection, even without power by using a backup battery. It will be designed to provide protection against all PCI PED physical attacks, including Differential Power Analysis (DPA), Temperature Variation (freezing of the device), frequency-based fuzzing, and physical access to the system memory contents.

Known Challenges

Aside from the required sensors, battery backup and the rest of the HW layout, it's important that the sub-system will have a negligible probability of false alarms that would lead to data wiping by accident (for example, when the device is dropped on the ground).

1.2. Physical tamper proof periphery - keyboard and display

Similarly to the computer itself, all peripheral devices must be packed in a hardened 'shell' that would prevent installation of additional hardware (loggers, microphones etc.), damage to the device and interference with the encryption/decryption component on board.

1.3. Encryption key separation

A separate dedicated device (based on a smart card) will be used for both user authentication and cryptographic keys management. It acts as a basic physical key containing cryptographic data. This is an integral part of the computer.

1.4. Secure firmware (UEFI)

Developing UEFI based firmware to minimize the attack surface and enable a trusted and signed OS boot. The firmware will prevent any form of legacy boot mechanism as well as a non-signed OS boot. This is performed by checking and authenticating the OS software to avoid the presence of malware and the conditions for loading. Generally speaking,

good design practice such as a lean BIOS, with state of the art security techniques improves the firmware defense against multiple types of attacks.
The UEFI will have an optional remote attestation features to enable additional features such as remote wiping, remote-authorize bootstrapping and more.

Known Challenges
The UEFI should be written well to avoid any potential compromise.

1.5. Secure Bootloader
A specially designed UEFI bootloader will be developed, further enhancing the boot process to enable cryptographically authenticated boot process based on a client provided key as well as destructive cryptography in case the device is compromised and data needs to be completely wiped in an extremely urgent manner (e.g. given a remote command from the servers to do so).

1.6. Signed OS
OS signing will be based on client provided keys (as opposed to vendor provided keys). It is likely that the signing process will be executed based on one of the existing technologies in the market, such as Boot Guard.

1.7. Secure Output
Creating a means of displaying content on screen which is secure against screen grabbing, recording, tampering and so forth. Assuming there is a frame to draw on the screen which originates from an enclave, the frame will be encrypted within the enclave and transmitted via a protected media path (OS level API) to the graphic driver. PMP encrypted frames cannot be decrypted by the OS and are decrypted by the (signed) display driver on a dedicated hardware in the graphics card.
An extension to this scheme is offering an HDCP-Like solution where the SGX encrypted frame will be deciphered only on the actual display.
This scheme offers enhanced security (with the requirement for a dedicated, specially developed display).

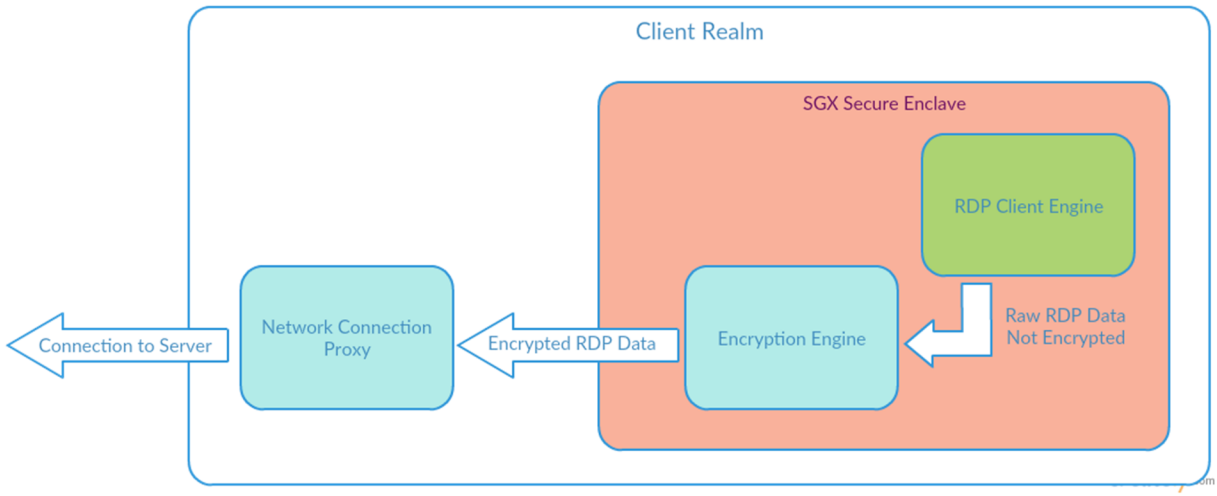
1.8. Secure Input
Creating a truly secure HID which is cryptographically secured against keylogging of any type (hardware, software, physical tampering, memory scraping and so forth).

Known Challenges:
When developing a secure keyboard there are several constraints and limiting factors. For once, the code on the HID must be protected too (assuming ARM's trustzone as a viable solution, while others are being examined).
Secondly, considering the extremely low resources embedded hardware (the kind being utilized on HIDs), developing a zero-latency encrypted channel with strong cryptography is highly challenging. The team is currently looking at the benefits that Elliptic Curves Cryptography (ECC) may offer in regards to resource-constrained embedded systems coupled with embedded-GPU based cryptographic code. Following the potential flaws of using ECC, including the sensitivity to proper key generation and NIST recommendations from the last year to avoid it due to potential future breaks, this is not the only relevant

option.
Lastly, the driver on the host side can be mostly regarded as “general software” development, using the SGX instruction set where needed. However, developing with SGX is highly challenging since it has major limiting factors due to its nature (small consecutive memory space for enclave, no Syscalls, severely limiting IO and so forth).

2. Client Software

The BIRD project will be the first software-hardware platform to fully utilize SGX on a secure platform, this will include both the RDP client and server, SGX Aware cryptographic library and authenticated peripherals. Having both within the SGX protection is a key factor in ensuring a safe and secure environment. The Network Connection Proxy (NCP) enables decoupling of the application code from the network code.
This has two main advantages:
1. It enables the user/organization to choose whichever transport suite they require (IPSec VPN, SSL VPN, ProxyChains, TOR, or even plain unencrypted connection)
2. It breaks the reliance of the application data security on the transmission line’s security, meaning the application data is self-protected.
Should the client use a secure transport (e.g. a VPN) it would add to security even further, but won’t be the sole contributor to it.



Main Elements:

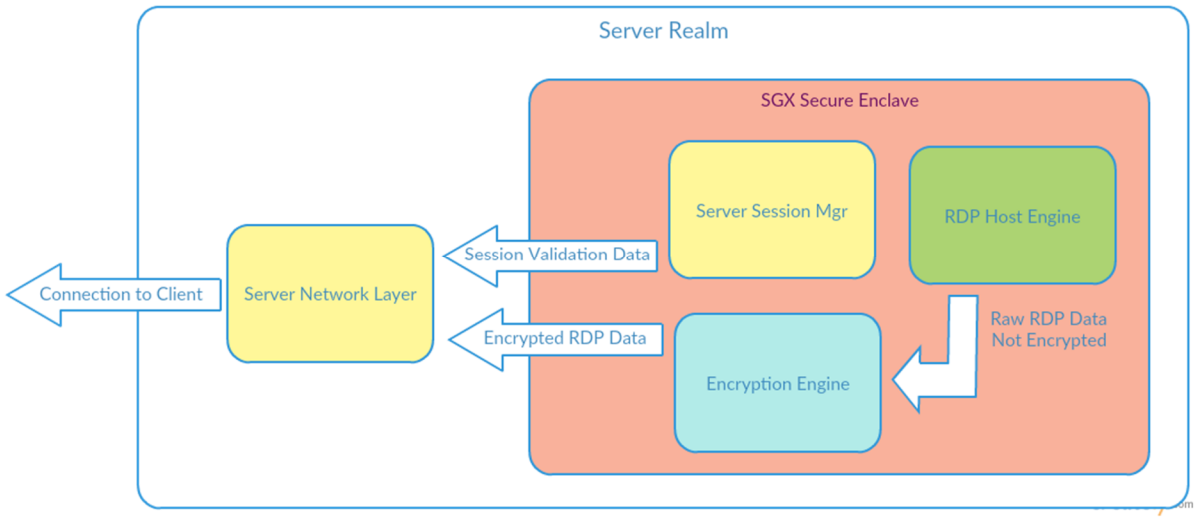
1. RDP Client Engine running within the SGX Enclave is responsible for handling user input and the RDP session.
2. SGX Aware Cryptographic framework providing encryption/decryption/authentication/signing and other cryptographic semantics.
3. Network Connection Proxy responsible for sending and receiving data and establishing server connection and session.
   This effectively creates a loose-coupling architecture between the transport layer and the application layer enabling user to communicate on any medium he wishes without affecting the security and integrity of the data, indirectly enables the user to augment the baseline protection with additional characteristics such as re-encrypt proxy, anonymity, ProxyChains and so forth.

Known Challenges:

- UI responsiveness and overall latency - will need to be addressed to make sure the cryptographic operations will have a minimal effect on the system's response and overall user experience while still maintaining resilience against different cryptanalysis attacks (which is directly derived from code optimization).
- Resilience to attacks on the cryptographic frameworks - thorough tests from documented cryptanalysis specifically targeting cryptographic semantics (e.g. side channel attacks, use-after-free, PRNG attacks, etc.), handle and fix every vulnerability that was found during testing.
- Technology - SGX severely limits application design and implementation (e.g. limited to non-existence Syscalls, lack of integrity with 3rd party libraries, etc.). Some limitations may pose a security risk and need to be addressed when developing (e.g. contiguous memory allocation, non-time-uniform ops).
  Currently, there's no support to several processor capabilities (EPA, VT-x, etc.) which poses significant challenge developing SGX-aware applications.

3. Backend Server Software

The backend server of the system will be the first of its kind, being SGX-based and therefore presents an innovative implementation of the SGX technology, which provides complete privacy and ensured trust.
The SGX-based code will securely import the customer's private encryption key, which is securely stored in a hardware smartcard at the endpoint, this key will be used to decrypt the user's data.
One of the major challenges will be to enable a working system under the assumption that the system is under attack. Since discovering an attack on the system (such as Trojan horse) could take a long time, the platform will need to enable consistent work assuming and dealing with attacks at the same time.
There is an additional challenge involving the Hypervisor. The platform will have to ensure it will not be used by the attackers as a tool to attack all the virtual computers in the servers' farm.
Another scenario which have to be prevented is one in which a Hypervisor's malicious manager will use his power to invade the computers in the servers' farm. For example - an employee that decides to perform illegal actions, or a malware that exploits the Hypervisor. Today there is no technology which provides full security over the virtual computer and allows zero trust on the cloud supplier. The technologies today offer partial solutions and secure only specific parts, such as: secure data storage, encrypted chats, VoIP etc.
In the course of this project the companies will develop the first solution that offers a full and complete protection of data on the client side, organization's system and the cloud.



Main Elements:

1. RDP Host Engine running within SGX Enclave responsible for providing remote RDP session
2. SGX aware cryptographic library.Cr
3. Server Session Manager running within SGX Enclave responsible for receiving client requests, validating credentials, SGX validity and creating user session
4. Server Network Layer responsible for sending and receiving server data
5. The server should also allow for import and export of data as most customers wish to be able to use some sensitive information in 'black' environments. The import and export mechanisms will be developed in a later stage of the project and will be modular with respect to the rest of the product.

Known Challenges:

- Scalability - deliver fully secured environment that can grow as demand grows, secure Hypervisor and SGX scaling
- Technology - SGX has severe limitations and it is not yet clear what is the best implementation of SGX on VMs within the server.
- Client authentication and validation - secure validation of every client session and request
- Resistance to attacks on the cryptographic frameworks - thorough tests from all known attacks including side channel attacks, handle and fix every vulnerability that was found during testing.
- Import and export mechanisms are a major challenge due to the transfer of data between 'red' and 'black' environments. This will be researched further in a later stage of the project.

4. Connectivity with the 'shell'

Handshake processes between the keyboard or display and the host are similar in some regards to TLS handshake, exchanging symmetric keys over, for example an ECC scheme.

A one-way handshake scheme will also be developed (meaning the keyboard will offer the symmetric key as well as any other cryptography dialect setup. While this is generally a simpler approach (and is preferred when writing HID) it prevent the host from specifying secure channel characteristics. The secure channel is used for symmetric keys exchange.

Once symmetric keys are exchanged (between ARM's trusted zone an SGX enclave) HID and the computer can exchange encrypted keystrokes protected from SMM/Ring0/Driver/OS compromise as well as physical keylogging and even induction eavesdropping.
The secure process running under an SGX enclave should route keystrokes according to a given logic between different enclaves (supporting re-encryption) as well as routing of keystrokes to a non-secure process (e.g, OS HID driver).

By tackling all of the abovementioned challenges the product will meet the full scope of specifications and requirements:

1. Fully secure system that reaches the benchmark of Pen-testing by highly skilled attackers and leading attack organizations without failing within a significant time frame.
2. High-end usability that includes low latencies, a pleasant and convenient user experience and a foolproof system.
3. Meeting all of the the standards that are described in chapter D of this document.
4. The capability to establish and expand a full manufacturing line while maintaining it secure and meeting the required standards and guidelines.

E2. Proposed Approach

General Plan Description

As a multi-disciplinary project with hardware, software, firmware and cloud components, the development consists mainly of creating components as building blocks on several levels and integrating them into a full device. After integration, comprehensive quality assurance, pen-testing and cryptanalysis will take place to benchmark and approve the result. It should be stressed that confirmation, testing and red-teaming are an on-going part of the development process, but full testing can only be performed once a prototype is ready.

The program includes the following:

1. Developing a user's end-point that includes a pocket computer and a 'shell' (keyboard, display and other interfaces), including all hardware and software essential components.
2. Developing a layered cloud solution, namely infrastructure, a trusted Hypervisor/Container, Secure storage, and Client session management software.
3. Integration of a prototype device
4. QA, Security/Risk assessments, cryptanalysis and Pen-testing

Development Methods

The development approach includes at its essence the wish to develop a unique product with outstanding security features, meaning that crucial systems and elements that may contain relevant trade-secrets will be developed in-house within the companies. The two complementing guidelines of the approach aim at preventing an over-complicated and perhaps unfeasible project – Using KAZUAR's existing technologies, assets and experience as tools to converge to a better result quicker. While at the same time, when an industry golden standard exists, supplies sufficient security and can be integrated into the system without potential harm, such solutions are carefully chosen and are fitted to the product.

The development guidelines and methodologies heavily rely on the significant expertise that both companies hold – KAZUAR has already completed the development, launch and performing sales of an operational product with some similarities to the one presented herein, and with some overlapping technologies and concepts. KAZUAR has a unique knowledge in system design and engineering for superb security as well capabilities and knowledge in fields of software and hardware coding, and the combination of cyber-security and physical security. Patriot has both the expertise and experience in developing hardened and secure hardware meeting the highest standards and beyond, for both the private as well as the security governmental sectors. The combination of the uniqueness of the two companies completes a wide expertise in the required security disciplines.

In addition to the aforementioned guidelines, the project has several parts that are beyond the expertise in either one of the companies, and is aiming to both maintain relatively low costs, and aiming to reach a production line that is capable of providing large numbers of units. Consequently, partners or main subcontractors are chosen to develop external parts such as a keyboard device that will be defined and integrated with encryption and tamper-proofing capabilities.

Detailed Description of Tasks

The development tasks of this project are as follows. After the tasks list, we present a detailed description of each one of them:

1. Client Side 'Red' Secure Environment
2. Development of a Secure Pocket PC
3. Main CPU Firmware
4. Development of the end-Point 'black' OS software
5. Development of physical tamper-proofing tools for all components
6. Development of a keyboard device
7. Development of a display device
8. Development of cloud software - secure storage and execution
9. Development of a secure import mechanism
10. Development of a secure export mechanism
11. Integration of a prototype device
12. System QA
13. Cryptanalysis
14. System Pen-testing
15. Certification

We present the tasks as measurable building blocks that comprise of multiple technological design and manufacturing sub-tasks. The tasks are presented in a semi-chronological manner, meaning that some of them will be performed in parallel as shown in the GANTT chart:

1. Client Side 'Red' Secure Environment

Task Description

Creating the secure environment that includes the client's front end and functionality to serve as a full desktop, storage, and internal communications within an organization's 'red' system. The initial code will focus on creating a system-wide cryptographic framework which will be the basis for all cryptographic semantic in the entire product (including SGX-aware client and server components, embedded derivatives with uniform APIs and same-level code correctness and so forth).
The cryptographic framework is a critical key component in the entire solution and strong emphasis will be made to ensure a tight integration for all components.
Other subtasks include a full SGX aware SSL-VPN for data access, an alternate generic tunnel service (for loose-coupling between data encryption and transport layer security), RDP for the client working environment and functional applications and secure input and output from the system.
This task will be led by KAZUAR, and a team of experts in the field.

Sub-Tasks

a. Cryptographic Framework
b. Code infrastructure, UI

c. SSL-VPN secure connection
d. RDP code

Subcontractors
Patent & IP Consulting

Complexity and Innovation
The main complexity in building a secure working environment is the tradeoff between the required high level of security and the wish to achieve a convenient user experience with low latencies. The system needs to apply the most up-to-date knowledge in cyber-security, and present simple interface to system administrators that will run it to control storage, permissions and users. For example, in building the Key Management System (KMS), proper care should be given to generation events, communications between components and to proper key exchange.
As a major aspect of the cryptographic framework, all decisions and implementations should be kept modular and aim for agile cryptography, with the option of replacing bulks of the implementation in case a cryptographic flaw is discovered (e.g. in an academic paper) or when different requirements are required (e.g. RSA instead of ECC, export grade restriction, client provided implementation and so forth). Constructing the cryptographic framework in an agile, configurable and decoupled will allow for quick adaptation when changes are required, or an improvement is available.

Schedule
Start month - 08/17
End month - 01/18

2. Development of a Secure Pocket PC
Task Description
Creating a prototype of the PC motherboard with all of its components. This task is the major one as it includes defining, designing and developing the hardware of the main end-point's component. The concept behind this task is to take an existing Pocket Computer and redesign it to fit the security requirements, and include all authentication mechanisms, secluded 'red'/'black' working environments, network connectivity and physical tamper-proofing. A leading example of the base system that can be used for this purpose is Intel's STK2mv64CC system on chip, and integrating it with a cellular modem, smart-card reader, and physical tamper defenses. The implementation requires both software and hardware development of multiple elements such as a secure UEFI firmware and all of its functionalities mentioned in previous chapters.

This task will be led by Patriot, including board design, components' integration and testing. KAZUAR will supply requirements and assistance with specifications, choice of components and system design.

Sub-Tasks
a. System architecture and choice of additional components
b. Board design and layout based on an existing board
c. Components integration

Smart-card based encryption keys separation
Biometrics

d. Board testing

Subcontractors
Industrial design
CTX tests

Complexity and Innovation
The main complexity of this task is designing a safe board, that does not present any security breaches, under the form factor and price constraints. To the best of our knowledge, such a system of a hardened pocket-PC does not exist as of today, hence, the design itself is completely innovative.

Schedule
Start month - 08/17
End month - 07/18

3. Main CPU Firmware

Task Description
To complement the previous task of creating the PC's hardware, a full firmware suit needs to be written. The firmware performs the essential tasks to initiate an OS (local or remote), handle secure input and output.
One of the key requirements is to completely remove any so-called legacy features (aka BIOS Support) to prevent potential attack surfaces while also introducing high-end security features such as destructive mechanism in case of a compromise, an optional remote attestation and remote wipe feature to prevent the system from booting without remote authorization, a UEFI signed bootloader and so forth.
This task will be performed by KAZUAR. Patriot's teams will advise regarding implementation and interfaces with hardware.

Sub-Tasks
a. UEFI development
Firmware development
Destructive cryptography
(Remote) Attestation process
b. UEFI Secure boot-loader code and components development

Subcontractors
Patent & IP Consulting

Complexity and Innovation
Writing the UEFI firmware including the implementation of all of the security components, running only own or trusted code is challenging. Design should be executed from near-zero assets, and coding should be performed well to avoid security breaches. In addition, the system architecture and implementation must be performed in a way that prevents compromise of any known type, and specifically allow secure input and output to the 'shell'

components through an encryption mechanism, and allowing continued secure work even when a part of the system was compromised, but does not allow an attacker access to sensitive information.

Schedule
Start month - 11/17
End month - 05/18

4. Development of the End-Point 'Black' OS Software

Task Description
The local OS serves to act as the local 'black' system in front of the user. It needs to communicate with the peripherals and be able to receive and decrypt information from peripheral components and communicate with the Internet. It should be designed to be highly secure, as well as compartmentalized from other parts to allow the continuation of sensitive data security in case it is being compromised. This tasks in its core is wrapping an existing OS with safety mechanisms.
This task will be led by KAZUAR. Patriot's teams will advise regarding implementation and interfaces with hardware.

Sub-Tasks
a. Safe OS mechanism
b. Compartmentalization solution
c. Ghost image loading
d. OS signing
e. OS updates mechanism
f. Client software and applications

Complexity and Innovation
Creating a safe operating system that will prevent malware manipulation at its own level, while on the other allow updates for both safety as well as usability is highly complex. This means that the system should be able to receive periodical updates, verify them and prevent usage of tampering or breaches in them.

Schedule
Start month - 04/18
End month - 08/18

5. Development of Physical Tamper-Proofing Tools for all Components

Task Description
To complement the cyber-security level that is achieved by using a holistic hardware-software-cloud, the development has to include a physical anti-tampering mechanism. There are multiple mechanisms that need to be incorporated into several components and names all of the physical parts of the system.
This task includes the analysis and marking of critical points that can be interfered within each hardware component, choice of build materials and mechanical components that aim at increasing the physical hardness and the design of a protection system that detects a penetration trial and wipes critical information from the device. Among the specifications and

scenarios, the system can operate regardless of a power source and to detect tampering trials on itself (changes in temperature, small breaches in package etc.).
This task will be led by Patriot, and using the company's extensive experience in creating hardened hardware systems. KAZUAR will aid in determining specifications and apply design ideas as part of the task.

Sub-Tasks
a. Recognizing key weak points and potential breaching points.
b. Definition of a mechanical protection suit including materials, adhesives and mechanical connections.
c. Design and development of a sensor unit that is separate from the main CPU and is independent of power supply.
d. Implementation of destructive cryptographic mechanisms

Subcontractors
Patent & IP Consulting

Complexity and Innovation
Physical tamper-proofing requires to both meet the highest levels of standards, innovate and keep some of the information as a trade secret to set the bar for undetected penetration as high as possible. Among other, the physical tamper-proofing needs to detect penetration attempts, including attempts to penetrate and overcome itself. It needs to do so under physical attacks as described above.
In parallel to this, the device needs to avoid false alarms in the tampering detection, that would result in rendering itself unusable. This means a wide variety of cases that include experiencing high accelerations from falling, natural changes in temperature and potential EMI.

Schedule
Start month - 1/18
End month - 8/18

6. Development of a Keyboard Device

Task Description
Development of a keyboard product that follows the design concepts, meaning interfaces with the user and transmits only encrypted information to an SGX enclave, with minimalistic on-board storage, only holding required functional code. The device needs to be developed in a way that fits both the CPU code and drivers, as well as implement the tamper-proofing. Special care needs to be taken when developing the encryption code: such peripherals usually have extremely low computational power and memory space which are severely limiting the cryptographic code.
This task will be led by Patriot, and using the company's extensive experience in creating hardened hardware systems. KAZUAR will aid in determining specifications and apply design ideas as part of the task.

Sub-Tasks
a. SoC/Microcontroller verification

b. Trimmed-down encryption micro-library with necessary changes to fit extremely low end compute units.
c. Client side OS's pseudo-driver code
d. Mechanical design
e. Integration and testing

Subcontractors
Patent & IP Consulting
Industrial design
CTX tests

Complexity and Innovation
The keyboard should be designed in a way that does not allow any manipulation or tampering by physical or cyber presence on any accessible parts, and specifically the prevention of key logging by adding a device to it. It needs to use the limited computational resources in an efficient way to maintain low latencies. An example of the result of the aforementioned tradeoff is the potential use of asymmetric encryption for safe key exchange and the use of symmetric encryption for ongoing communications using limited computational resources.

Schedule
Start month - 11/17
End month - 07/18

7. Development of a Display Device

Task Description
Development of a peripheral device that allows display for users' interaction. The component needs to be designed in a way that is fully functional and convenient in terms of low latencies, while supplying security against screen grabbing. This task includes the mechanical, electronic and software development.
This task will be led by Patriot, and using the company's extensive experience in creating hardened hardware systems. KAZUAR will aid in determining specifications and apply design ideas as part of the task.

Sub-Tasks
a. System design
    Base hardware validation
    Core Development
    Client side (i.e. SGX-PAPV bridging)
b. Base device verification
c. Client side OS's pseudo-driver code
d. Mechanical design
e. Integration and testing

Subcontractors
Patent & IP Consulting
Industrial design

Complexity and Innovation

All parts of the ‘shell’ should maintain low latencies in the user experience in spite of the limited computational power. The display unit must be designed to meet the highest standards of hardware security to prevent data leakage by screen grabbing, even in the case of the implantation of an additional device on the display itself.

Schedule
Start month - 11/17
End month - 07/18

8. Development of cloud software - secure storage and execution

Task Description
Develop a zero-trust secure execution environment, e.g. Zero-trust hypervisor or Zero-trust container technology (e.g. Docker, Rocket, BHive, Jails etc.), including all of its functionalities, multiple secure VM handling, security and key handling for all communications.
This task will be performed by KAZUAR.

Sub-Tasks
a. SGX server-side implementation research and design
b. Hypervisor
c. Communications handling

Subcontractors
Cloud Security Expert
Security Expert
Cryptographic Consulting Review

Complexity and Innovation
To the best of our knowledge, this is among the first systems that offer customers to have privacy from the vendor. A major part of the security and privacy results from the use of SGX technologies, that were not used before to fully implement back-end systems. The first generation of SGX does not allow for this to be performed in multiple parallel guest VMs. This can be worked around as a first step with different servers and a gateway that reroutes traffic to the relevant server, and will be solved completely with the next soon-expected generation of Intel’s SGX.

Schedule
Start month - 08/17
End month - 07/18

9. Development of a secure import mechanism

Task Description
Develop the ability to export or at least import information into the ‘red’ environment. Such activities opens the gate for either a system compromise or information leakage. The development includes the relevant software for permission handling, AV integration and logging and the hardware for data transfer.

This task will be performed by KAZUAR.

Sub-Tasks

a. Secure import mechanisms research
b. Implementation of multiple existing AV tests, disintegration of files, removal of execution files etc.
c. Implementation of physical gateway
d. Integration and security testing

Subcontractors

Patent & IP Consulting

Complexity and Innovation

Any import action of data into a secure system presents a potential security breach. This sub-system needs to be designed in a way that would limit the potential harm and still enable users to import information given relevant permissions and following the required tests.

Schedule

Start month - 07/18
End month - 02/19

10. Development of a secure export mechanism

Task Description

Developing an export mechanism that would allow using 'red' data in external devices including printers and transfer to 'black' systems. The system needs to allow for strict permission management and fault prevention, monitoring and logging. As part of this task, comprehensive research will be conducted regarding implementation alternatives.
This task will be performed by KAZUAR.

Sub-Tasks

a. Secure export mechanisms research
b. Automated tools for stripping metadata
c. Permission control system
d. Integration and security testing

Subcontractors

Patent & IP Consulting

Complexity and Innovation

Any secure export system is problematic due to the nature of sending data out of a sensitive information system. Integration of an export system needs to be performed with extreme care to potential backdoors and breaches.
The need to avoid any sensitive information leak through files' metadata is specifically challenging and requires proper care and designated solutions.

Schedule

Start month - 07/18
End month - 02/19

11. Integration of a prototype device

Task Description

Taking all of the building blocks that were described in the prior tasks and integrating them into a functional prototype of the device which includes both hardware and software components, including the remote connectivity to secure servers. This task will be mutually performed by both companies integrating Patriot's hardware with KAZUAR's software.

Sub-Tasks

a. Integration of all hardware components into a user's product
b. Integration with servers

Complexity and Innovation

The complexity in this task arises from the need to connect multiple different system, that will in all likelihood require fixing and improvement during integration. As no such system exists today, integration in a way that will not create any security breaches is complex and potentially risky. All this in parallel to the requirements for usability and reliability.

Schedule

Start month - 09/18
End month - 03/19

12. System QA

Task Description

The integrated system is being put through software, hardware and usability testing to reflect its functionality, prevent errors and find system limitations and constraints. It should be noted that testing is an inherent part of every task in this program, and this task refers only to the QA intensive process for the entire integrated product.
This task will be mutually performed by both companies.

Sub-Tasks

a. Developing testing infrastructure
b. Automated testing
c. User testing

Complexity and Innovation

As this project's product is a first of its kind and includes multiple complex components, quality assurance processes are expected to be complex and errors might arise and need to be fixed in a manner that does not present any security breaches.
The testing should be thorough and check both functional limitations in usability, connectivity, scalability and others.

Schedule

Start month - 11/18
End month - 08/19

13. Cryptanalysis

Task Description

Assessing the correctness and resilience of cryptographic products based on external domain experts, automated tests with designated tools as well as specific attacks against cryptographic framework as published in peer-reviewed research/literature.
Due to the high importance and potential flaws in the cryptographic implementation, a comprehensive research task is dedicated to checking the robustness in face of relevant threats and state-of-the-art academic knowledge in the field.
This task will be performed by KAZUAR.

Sub-Tasks
a. Cryptographic testing and analysis

Complexity and Innovation
The innovation in the task arises from the need to protect against attackers with extreme decryption capabilities and enormous computing powers. This means that the cryptographic framework and its testing should be sound at the highest level.

Schedule
Start month - 02/19
End month - 05/19

14. System Pen-testing

Task Description
Testing of an integrated device to benchmark its security level and recognize if weak points can be recognized and fixed. This in stages in which world renowned experts and organizations with attack capabilities are being given the system and asked to try and compromise it or part of it. As part of this task, and to ensure the customers trust, a committee comprising of world-renowned experts with experience in both defending and attacking systems, will be assembled and used to find potential weak points.

It should be noted that Pen-testing is an inherent part of every part of this program and this task refers only to major testing of the integrated full device. We plan to conduct two major sessions of Pen-testing, one at approximately the middle of this program, with initial integrated prototypes, and the other towards the end of the program with the full system.
This task will be performed by KAZUAR.

Sub-Tasks
a. Initial testing of first prototypes
b. Comprehensive testing of final product

Subcontractors
Pen Testing company

Complexity and Innovation
Pen-testing should be performed in a thorough way by unbiased teams of experts that work

together to find breaches and faults in the system's security. Although this is not an innovative concept by all means, the requirement for thwarting attacks by governmental espionage organizations sets the bar for this task at a level that demands superbly complex Pen-testing.

Schedule
First phase:
Start month - 01/18
End month - 05/18
Second phase:
Start month - 09/18
End month - 01/19
Third phase:
Start month - 03/19
End month - 07/19

15. Certification

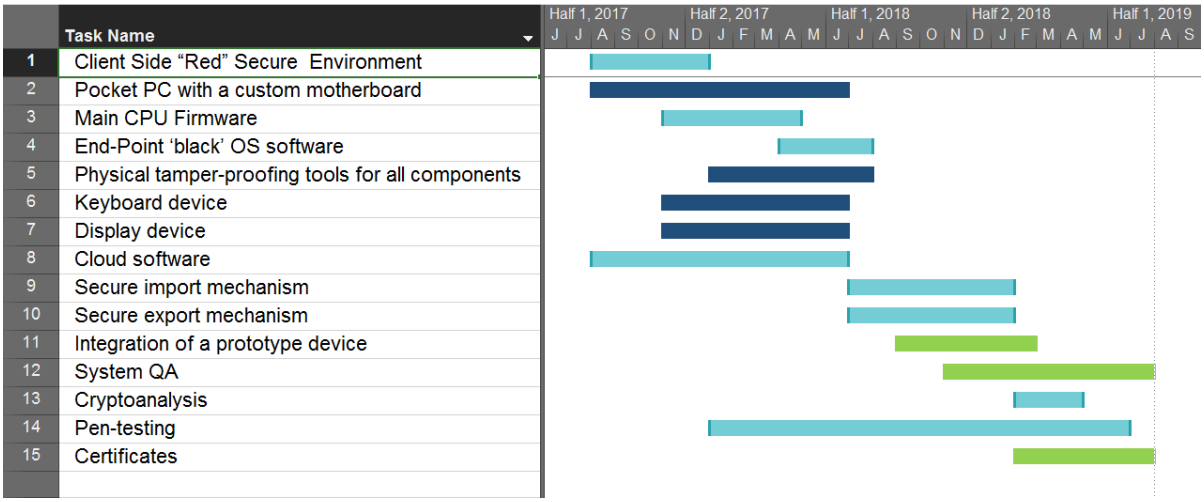
Task Description
The full system needs to be certified to meet the highest standards of security and quality. Among others it should be certified by relevant third parties to the hardware and software security standards by NIST, the European Committee of Standardization (CEN) and the Standards Institution of Israel (SII).
Among others, the full system is required to meet FIPS 140-2 level 3 and 4, PCI, HIPAA, ISO 27001, and ISO 27799. The certification of Common Criteria is not within the scope of this program due to long required periods. It is however, a long term aim of the companies.
This task will be performed mutually by KAZUAR & Patriot.

Subcontractors
Global Certifications
FIPS consulting and US certifications

Complexity and Innovation
This task presents one of the entire development program's results, hence its complexity arises from the multiple prior tasks and the need for proper design, documentation, execution and integration. The design of industrial manufacturing processes and administrative processes such as working procedures and regulations is also crucial to reach the required level of standards.

Schedule
Start month - 02/19
End month - 08/19

F. Program Plan



G. The Market

G1. Market Background

The outcome of this BIRD project is an intelligence-grade security solution designed for non-IT experts. Therefore, its potential market will be composed of organizations holding sensitive and valuable information:

1. Business organizations or specific department within the organization that manage confidential data such as financial bodies, insurance companies, manufacturers, security contractors etc.
2. HNWI – individuals, owners of sensitive information or expensive properties.
3. Government organization such as intelligence, security, international communication etc.

As the volume of information held by organizations today is increasing, information become more valuable and sensitive. Attackers on the other hand are becoming more complex and sophisticated, and organizations are forced to confront governmental-level cyber-attacks. As a result, organizations these days seek high-end reliable **cloud security** solutions. Moreover, since the developed solution will be designed to be user-friendly for non-IT experts, it will be fit even for small organizations with no IT departments that require high-end security for their data.

Cloud Security Market Review

The market today

According to FORRESTER's survey from October 7 2015, 34% of North American and European business decision-makers at Enterprises today use software-as-a-service (SaaS) applications in their group or department, and another 24% plan to do so in the next 12 months. However, even as cloud adoption is accelerating for software, organizations today are very concerned about the risks that could be introduced to their firms by moving their sensitive data such as customer data, employee data, intellectual property, to the cloud.

Data security has become essential to building and maintaining customer relationships. If a firm uses cloud services, ultimately, it is responsible and liable from a legal perspective for protecting its customers' data, particularly in regulated industries such as banking, healthcare, and the public sector.

Nonetheless, preserve privacy and achieve compliance in the cloud become very challenging today. S&R pros struggle to inventory, classify, and protect the sensitive data stored in the laptops, desktops, and data center infrastructure they claim they can control.

According to Forrester, the top three most common ways in which breaches occurred:

1) internal incident within their organization (46%)
2) external attack targeting their organization (33%)
3) external attack targeting a business partner/third-party supplier (32%)

Therefore, it's not just the external attacks or the malicious insiders that the firms have to worry about, it's also a cybercriminal attacking their provider or the internal employee of their provider maliciously or inadvertently misusing data.

Traditional perimeter-based security solutions, such as VPN-based network access controls

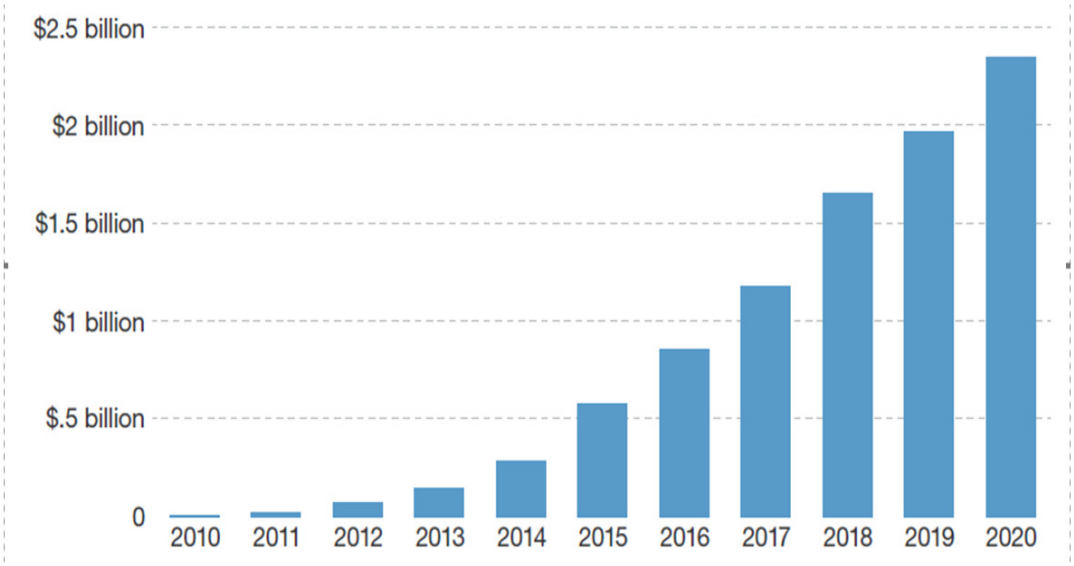
and security information management, do little to protect cloud workloads because vendors designed these solutions so that S&R pros could monitor corporate network traffic for malicious activity and malware, even networks these days become far less relevant as organizations transferring their sensitive data to the cloud.

Market prediction

Forrester predicts that spend on cloud security solutions will grow at a compound annual growth rate (CAGR) of 42%, from $282 million in 2014 to more than $4.6 billion in 2022. Implicit in that analysis are the assumptions that:

- Cloud security will grow in line with public cloud and virtualization adoption. Customers purchase cloud security solutions before, during, or after implementation of cloud-based technologies. Generally speaking, the market for cloud security should grow at least as fast as that of cloud technologies as a whole. Given that the market for public cloud platforms will grow at a six-year CAGR of 34%, and the SaaS market will grow at 14%, we view our forecasted 42% annual growth rate for cloud security to be appropriate.
- S&R pros are increasingly interested in pure-players to fulfill their cloud security requirements. The need to innovate is gaining precedence over the legacy mindset that is plaguing stodgy organizations.
- 37% of enterprise execs spanning IT and business units report plans to increase security funding in reaction to the high-profile data breaches at organizations like Sony, Living Social, Adobe, and Target. A portion of this new funding will fuel the cloud security market. S&R pros must protect data in cloud workloads just as well as in on-premises workloads

Global cloud security solutions spending CAGR: 42%



G2. Costs and Pricing

The companies determined the prices while taking into account the manufacturing and recurring costs, so that the price would allow them to maintain high gross profit, exceeding 80%. The prices allow both profitability and significant business flexibility to provide discounts for strategic customers. It has also been considered that the product is essential and invaluable to its customers, who will do anything to protect their work environment from data

leaks. The system's costs are marginal to them compared to the potential damage they sustain in case of a data breach, and they are certainly lower than the accumulative costs for a customer that would try to integrate a similar solution from scratch, by himself.

The pricing model: SecaaS - Security as a service - based on one-time setup fee and recurring monthly service. This is the common model and it is attractive for most of the customers, who usually prefer flexibility and simplicity and avoid investment in infrastructure. At the same time, due to the nature of the solution, it creates a significant dependency of the customer and therefore provides us with a continuous cash flow.

One of the references for the two companies is KAZUAR's initial sales of its current solution. Both well-experienced re-sellers and end-customers approve of both the solution and the prices. Customers are using the system intensively and renewed the recurring payment. We believe that The sales projection is very conservative - both in terms of market penetration and prices. The projection's prices are based on the current prices, although the two companies are convinced that in practice prices will be significantly higher. The BIRD project is going to conduct a significantly better solution in a few aspects - security, mobility and user experience. It is a complete computer, and therefore will save the customer significant IT costs. A one time setup fee of $3,000 is cheaper than the power models of Microsoft's Surface Book, while Microsoft do not offer any unique security capabilities. In addition, a massive marketing campaign will be launched, while until now KAZUAR has been working "under the radar".

We aim at two different segments of the market: the premium market and a broader part of the market. The first one creates a major opportunity, since it allows very high gross profit. The latter allows significantly higher scalability, while still maintaining high profitability - although lower from the first.

The premium market includes 3 different kinds of customers:

- HNWI and related - businessmen, family offices, wealth management firms, hedge funds, law firms and accountants serving them
- The most important parts of corporations dealing with very sensitive information - management, R&D, legal department, M&A, etc. of manufacturers, financial institutions, insurance companies, security contractors, etc.
- Governmental organizations, mainly decision makers and security organizations

Since the premium market includes organizations dealing with top- secret information and in protecting major assets, they are willing to pay practically any price.
The broader market will allow us significantly higher scale, while maintaining high profitability. This market includes the following organizations:

- Complete organizations such as financial organizations, manufacturers, healthcare, insurance companies, security contractors, etc.
- Law firms and accounting firms
- Major industries, which are vulnerable to major cyber attacks, such as the automotive industry (one of the fastest growing industries) and the naval industry

The one-time setup-fees within the broader market (Secure PC Lite) will be similar to the one-time setup fee in the premium market, but in order to enable significant penetration to this segment, we will offer dramatically lower recurring service fees.

Cost:

	One Time Fee	Recurring Service
Secure PC Premium	3,000$	500$
Secure PC Lite	3,000$	250$

In addition to the comparison above with the Microsoft computers, our proposed recurring monthly fee is not higher than conventional MSP (Managed Services Providers) suites, which do not include any kind of special security features

The main barriers to market entry are the need to make organizations adopt a new technology that is not yet offered to them, and to have them understand a holistic approach to cyber-security. These barriers are overcome in several layers. Firstly, the product was designed and intended for seamless and simple integration into an organizational workflow, meaning the amount of habit changes is minimalistic, and convenience is kept at its highest. Secondly, and regardless of KAZUAR's and Patriot's actions, the demand for better cyber-security solutions increases, as defense solutions lag behind the increasing offensive capabilities. This means the market will seek solutions that are stronger and more robust, which will not only make the technology presented here more appealing, but in some cases the natural leading choice. Thirdly, we intend to leverage the innovation and paradigm shift in the approach into relevant public relations, that include the use of meeting the highest standards and the opinions of leading experts, within the development team and external to it. Lastly, instead of changing the way major customers handle IT, we intend to supply the solution to the IT providers themselves, hence giving them an incentive to work with the presented technology, and not to fight it.

As described in the competitive analysis, in the private market there are currently no direct competitors - no other company provides a solution that offers complete end-to-end security, with the ability to thwart state-backed attacks and with excellent user-experience. Theoretically, a customer can hire a dedicated team of ex-intelligence experts in various fields, conduct a threat analysis, engineer a custom-made design, write the code, manufacture certain parts and integrate dozens of parts. It might take him around 2 years, an investment of millions of US dollars and we doubt that he would get the same level of security we offer straightaway.

G3. Sales Forecast

Calendar year	**2020**		**2021**		**2022**	
The Solution Type	**Lite**	**Premium**	**Lite**	**Premium**	**Lite**	**Premium**
Target market size for developed product (M$)	2,312		3,283		4,662	
Estimated market share (%)	-		0.3%		0.8%	
Estimated sales quantity (units)	143	493	1,228	894	3955	2,509
Estimated representative unit price ($/unit) one-time fee	3,000	3,000	3,000	3,000	3,000	3,000
Estimated representative unit price ($/unit) Recurring Service per mount	250	500	250	500	250	500
Estimated sales revenue (K$) one-time fee	430	448	3,617	2,640	11,434	7,079
Estimated sales revenue (K$) Recurring service	218	429	11,896	3,138	9,649	13,246
Total Estimated sales revenue (K$)	1,525		11,291		41,409	
Total Estimated cumulative sales revenue (K$)	1,525		13,286		54,695	

H. Commercialization - Plans and Prospects

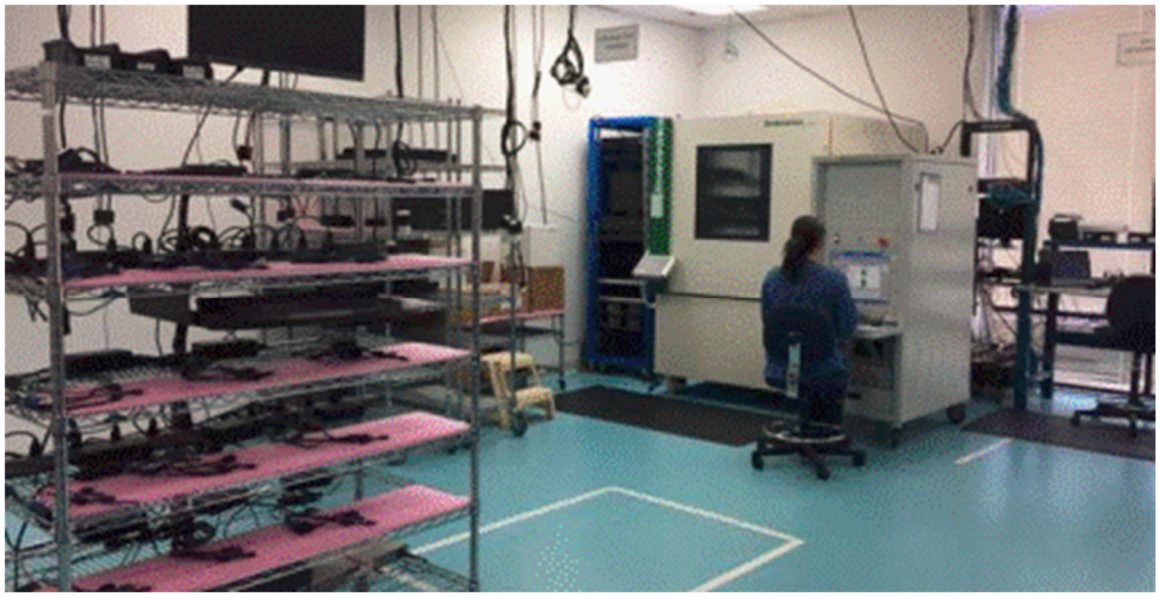
H1. Product Manufacturing, Marketing and Sales Activities

Product Manufacturing

Patriot Technologies will be responsible for manufacturing the hardware. Patriot is an ISO9001: 2008/2015 certified, Build-to-Print, U.S. manufacturer specializing in complex and precision products.

The company have more than 20 years of experience in platform development for world leading technology companies such as: Akonix Systemtec, Check Point Software Technologies Ltd., Cisco Sourcefire, Hexis Cyber Solutions, Imperva Secure Sphere, IBM ISS Proventia, Nokia, Saint, Tricipher protecting Online Identity, Skybox Security, Tenable network Security, Tufin, Ridgeback, Unisys etc.

The services of Patriot include: Manufacturing, Integration,Test, Environmental Testing, Quality Assurance, and Logistics services. Patriot is ITAR compliant and welcome FMF contracts and pass-through procurement for U.S. origin products, supporting military defense and intelligence programs to assist US and foreign initiatives. Patriot continues to apply its expertise developing programs for Security as a Service, Managed Mobility Services and innovative cyber security solutions to support a wide variety of mission goals and deployment strategies.



Marketing and Sales Activities

Patriot will sell the hardware devices that it manufactures to KAZUAR. Patriot will also commercialize the solution in the US as a non-exclusive distributer by using its well established sales and marketing infrastructure. Patriot has 20 years of experience in commercialization, sales and marketing, during which has worked with the most advanced technological companies in the world.

Financial resources & marketing capabilities

KAZUAR

KAZUAR has a definite capability to fund all of its part in the costs, both R&D and S&M. The company is in the final steps of a funding round, and has investor's commitment to invest funds that are significantly higher than required for the project. In any case, the founders and the current shareholders have an autonomous capability and willingness to provide the required funding. In the recent two years the company funded costs exceeding 2 million dollars, and managed to create a unique operational solution and start initial sales, while always keeping the company in positive balance. The company has never requested and have never been in any kind of debt and never requested any kind of credit.

Due to the attractiveness of the current solution and an efficient method of S&M, KAZUAR managed to start initial sales, despite the fact that it invested very modest resources in S&M at this stage, and had a very lean structure. At this stage, S&M were managed only by the CEO and COO, who of course have done it in parallel with other important missions and fields of responsibility. It was marketed “under the radar”, by identifying leading re-sellers, who has the required knowledge and connections to be able to understand and sell sophisticated cyber solutions.

In the vast majority of cases, the re-sellers have made a decision to make KAZUAR’s solution their preferred and sole defensive cyber solution. Sooner than expected, the company started receiving through them organic initial work orders, without any direct connection with the customers. Following a major security event in which the system prevented a major data leak that could have been destructive on a global level, the company received a letter of appreciation from the customer’s representative - Yohai-Bar-Zakai - who was the deputy commander of unit 8200

Due to the great potential of the BIRD project, in addition to the investment in R&D, the company is going to invest significant resources in S&M as well. The marketing and sales will be managed by a dedicated S&M director, and specialized directors in North America, Europe and the UK. All of the abovementioned with an exceptional experience in marketing and selling sophisticated IT and security products. KAZUAR is going to have physical presence in the United States and two important financial centers - Luxembourg and London and going to hire two leading marketing and sales firms: one of them located in Singapore and specializes in marketing to southeast Asia and the other one located in UAE, and specializes in marketing to the Gulf countries. In addition to those focused activities in the US, the UK, Asia and the Gulf countries, KAZUAR is going to extend its current fruitful cooperations with resellers, in order to reach out to additional re-sellers, either regional or with an added value in a certain important industry.

It’s important to note that one of KAZUAR’s new investors is a well-connected European fund from the financial sector, which has profound connections and infrastructure in Europe. They are going to be actively involved in providing offices, opening a European subsidiary in Luxembourg, running the regional marketing and sales operations and leveraging their connections, both with global banks and financial institutions and with European customers. In addition, in contrast to the “under the radar” approach until now, the company is going to leverage the uniqueness of the new solution, in order to present it in the leading global cyber security and technology conferences, and have allocated significant resources, in order to do so.

PATRIOT

Patriot is a 21 year old company with lines of credit and established financing capabilities. The company is currently in process of obtaining a new funding package in the $7M range. Patriot have lines of credit for all its vendors etc.

The company is active in the US market for all of this years and had work with many key factors in the relevant area. During the years Patriot created and maintained significant business relations with the world’s leading technological companies some of them can be potential clients to this BIRD project.

H2. Cash Flow Analysis

No.	Cash-Flow component	Derivation	N = No. of Years							
Y	Calendar year	Ist Calendar Year	2017	2018	2019	2020	2021	2022	2023	2024
	Project year		1	2	3	4	5	6	7	8
Q	No. of units sold (Units)	estimate			328	2,414	8,585	17,700	27,656	37,612
P	Product Price ($/unit)	estimate			4,647	4,678	4,823	4,681	4,508	4,382
S	Product Sales (K$)	=Q*P or estimate		0	1,525	11,291	41,409	82,862	124,671	164,824
M%	Manufacturing Cost (% of sales)	30%		30%	30%	30%	30%	30%	30%	30%
M	Manufacturing Cost (K$)	=M% x S		0	458	3,387	12,423	24,859	37,401	49,447
O%	Operating Expenses (% of sales)	28%		28%	28%	28%	28%	28%	28%	28%
O	Operating Expenses (K$)	=O% x S		0	427	3,162	11,595	23,201	34,908	46,151
D	Development Expenses (K$)	estimate	600	1,600	900					
C	Capital Expenses (K$)	estimate								
E	Depreciation (K$)	linear over 5 yrs.	0	0	0	0	0	0	0	0
I	Before Tax Income/Loss (K$)	=S-M-O-D-E	-600	-1,600	-259	4,742	17,392	34,802	52,362	69,226
T1	Cumulative Losses carried over (K$)		-600	-2,200	-2,459	0	0	0	0	0
T2	Taxable Income (K$)		0	0	0	2,283	17,392	34,802	52,362	69,226
T%	Income Tax Rate (%)	25%	25%	25%	25%	25%	25%	25%	25%	25%
T	Income Tax (K$)	=T% x T2	0	0	0	571	4,348	8,700	13,090	17,307
OF	Operating Cash Flow (K$/Yr.)	=I+E-T	-600	-1,600	-259	4,172	13,044	26,101	39,271	51,920
W%	Working Capital (% of sales change)	25%		25%	25%	25%	25%	25%	25%	25%
W	Working Capital Change (K$)	=W% x (Sn-Sn-1)		0	381	2,442	7,529	10,363	10,452	10,038
V	Residual Value of Assets		0	0	0	0	0	0	0	41,206
AF	Total Annual Cash Flow (K$)	=OF-C-W+V	-600	-1,600	-641	1,730	5,514	15,738	28,819	83,087
CF	Total Cumulative Cash Flow (K$)		-600	-2,200	-2,841	-1,111	4,404	20,142	48,961	132,049
R	Annual Discount Rate (%)	15%								
DAF	Annual Discounted Cash Flow (K$)		-522	-1,210	-421	989	2,742	6,804	10,834	27,161
DCF	Cumulative Discounted Cash Flow (K$)		-522	-1,732	-2,153	-1,164	1,578	8,382	19,216	46,378
IRR	Inernal Rate of Return (%)	114%								

I. Cooperation, Economic and Social Benefits

At the beginning of 2016 KAZUAR made a strategic decision to create a cooperation with a US based secure hardware company who works with US security organizations. As an Israeli security company that has unique experience in threat analysis, offensive cyber-security and in designing highly sophisticated security systems, the company understood that, in the long term, the best partnership would be one that is US-based, and that specializes in manufacturing highly secured hardware. KAZUAR need a hardware manufacturer, because it is not their added value, and they had no reason to try and do that on their own. The company needed to work with a US-based company, so they can more easily comply with the US regulations, meet the requirements of the US government, build a reputation and trust in the US market, and be able to sell to the private sector and hopefully in the future - to the US government as well.

In the last few months the companies began discussing possible cooperation \ and got to the conclusion that it is a perfect match and a natural and strong synergy for the following reasons:

1. Professional synergy - KAZUAR have unique knowledge and experience in threat analysis, offensive and defensive cyber security, designing sophisticated and comprehensive defense systems and software development. Patriot has a unique knowledge and experience in secure hardware design and manufacturing, in complying with US and global hardware standards and certifications and in working for and with the US government.
2. The companies share common professional attitudes, concept and methods towards security and work processes.
3. Patriot has a very positive record of long-term cooperations with Israeli companies.
4. Management in both sides created a very good personal and working relationships.
5. We are both highly committed to this partnership.

When KAZUAR started the cooperation with Intel, Patriot were among the first ones to know, and were involved in the process of reviewing the SOW. We discovered then - again - that we have a strong partnership and commitment and that we are on the same page.as has been noted above, KAZUAR will be responsible for the development of the secure software (multi-layer security, encryption abilities etc.), define the technological features of the hardware components and perform prototypes system tests. Patriot will be responsible for manufacturing the hardware prototypes and performing a series of lab tests (e.g. pen testing and physical tampering), for the development of the hardware manufacturing process and will advise on aspects of American regulation. Both companies will jointly develop the hardware detailed design. The companies agreed that KAZUAR will hold any foreground IP of the developed technology, regardless of inventorship, and will receive all revenues. Patriot will sell the hardware devices that it manufactures to KAZUAR. Patriot will also commercialize the solution in the US as a non-exclusive distributer by using its well-established sales and marketing infrastructure.

This BIRD project will enable KAZUAR to make a significant progress towards the commercialization of the product name system, comply more easily with the US regulations, meet the requirements of the US government, build a reputation, and trust in the US market.

Patriot will benefit from the higher manufacturing quantities that the project may provide it and the new markets they will penetrate through KAZUAR. Additionally, it will enter the new

market of cyber security systems.

As a direct consequence from this project, both Israel and the U.S. will strengthen the relations between the countries and will benefit from the market penetration. Israel will achieve economic strengthening in the U.S. and will enjoy from deepening its international recognition for its technological capabilities. The U.S. will enjoy from new capital formation. For both companies, this collaboration will enhance their human capital, increase their economic potential and enable their growth and development.

J. Organization and Management Plan

J1. KAZUAR Personnel

One of KAZUAR's major assets is its diversified and experienced team. The company combines expertise and track record in strategy, security, management and branding. The technological team includes leading security experts from elite units in the Israeli intelligence agencies.

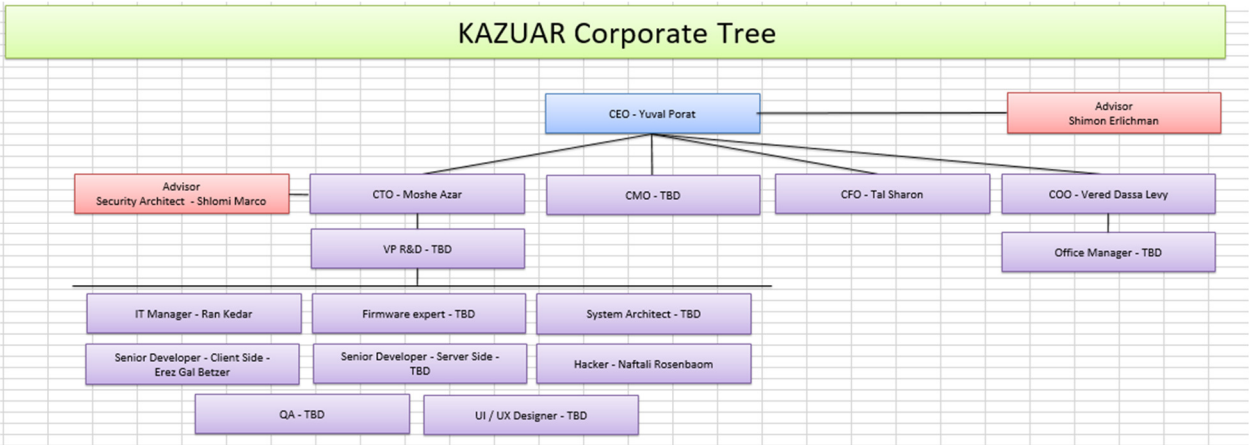
Yuval Porat – Co-founder and CEO - Has 20 years of experience and proven record in strategy design, crisis management, branding and communications. Throughout his career, he successfully managed highly complicated projects with global reach. He has extensive connections with major decision makers, among the private sector and governments.

Moshe Azar – Co-founder and CTO - Has a unique experience and proven record in data security, telecommunications and business management. For almost two decades now, he owns and manages a leading, highly successful IT company that designs and implements solutions for various complicated and sensitive mission critical projects around the world.

Tal Sharon - CFO - A consultant and an entrepreneur specializing in business development procedures in high-tech companies at various stages. Working previously as a Senior Accountant in Ernst & Young High-Tech Assurance Department and in Glusman & Co's Commercial Law Department. For the past few years, has advised start-up projects on different financial aspects.

Itamar Kunik - Board of advisors - 15 years of mobile & Telecom experience both in business and technological positions. Served at unit 8200 and has a unique experience both in cybersecurity and technology development. Serves as a CEO of a cash-positive startup and as a CTO of 60M+ subscribers' network.

Shimon Erlichman - Board of advisors - Spent 30 years in the Israeli security services, most recently as the CTO of one of Israel's key government security organizations. Shimon brings great technological depth and breadth of knowledge across numerous fields of science and technology. B.Sc. in Electrical Engineering from the Technion-Israel Institute of Technology.



Position to be filled by new employees:

VP R&D
CMO
Senior Developer - Server Side
QA
System Architect
UI/ UX Designer
Firmware Expert

Consultants and Subcontractors:
Pen Testing
Global Certifications
Patent and IP consultant
FIPS Consulting and US Certifications
Industrial Design
CTX test
Senior Architect
Senior Architect
Security Expert
Cloud Security Expert
Physical Tampering Expert
Security Expert
Cryptographic consultant review

Examples of persons acting as consultants in different fields:
Harel Menashri - Ph.D. in Information Science, Research Topic: "Integrating Cyber Warfare into Different Types of Warfare: The United States of America – Case Study". Served 36 years as part of the Israeli security system, including 25 years in the Prime Minister's Office in research, security and protection of critical infrastructure – both civil and defense complex systems (IT and SCADA) - from cyber, as well as other types of attacks, advanced technology application, incident and emergency response and more.

Shlomi Marco - Has a unique expertise in Intelligence systems for counter-terrorism and counter-espionage, big data, offensive and defensive cybersecurity and more. Served as Signal Intelligence system architect in IDF's elite intelligence unit 8200 and later served in the Prime Minister's office, while specializing designing, building and managing of national scale signal intelligence systems.

Be'eri Katznelson - has over 35 year of experience in creative mechanics problem solving and multi-disciplinary projects. He has unique expertise in multiple fields and vast experience in suggesting, implementing and scaling solutions. Among others, he is consulting regarding physical attacks and protection from them.

The following procedures will be implemented in order to maintain communications between each project's teams:

A. Timely meetings of team's management to validate budget and on time delivery. Meetings will be documented and reports will be sent to key stakeholders to follow-up on progress.
B. Integrated working meetings – according to need of relevant team members to keep track of schedule, set and track milestones, follow-up on previous action items and solve

specific issues in regards to integration and collaboration. Meetings will be documented and reports will be sent to team's managements to follow-up on progress.

C. Collaboration and information sharing tools will be used by all teams to share knowledge and enrich team members with other teams' progress.
D. Dedicated knowledge transfer Champion will be nominated on order to align all teams' to timelines and to overview budget and compare planning to execution.
E. Incentive team members to report on miss-matches and deviations from project's plan.
F. Mr. Shimon Erlichman was nominated by Company's CEO to overview and inspect integrated processes and to have a wide perspective of project's progress. Shimon Erlichman, who serves at the board of advisors, was the CTO and the deputy director of one of Israel's key government security organizations. He brings great technological depth and breadth of knowledge across numerous fields of science and technology.
G. The company will hire dedicated consultants to be used as 'Red teams' for the purpose of maintaining an overall due process, according to best practices aligned with project's plan.

See timely meeting Matrix:

	When	**Where**	**Purpose**	**Participants**
Management	Weekly	Company's office	validate budget and on time delivery	Team's managements
Teams	On Demand	Company's office	validate on time delivery and solve specific issues	Team members

J2. Patriot Personnel

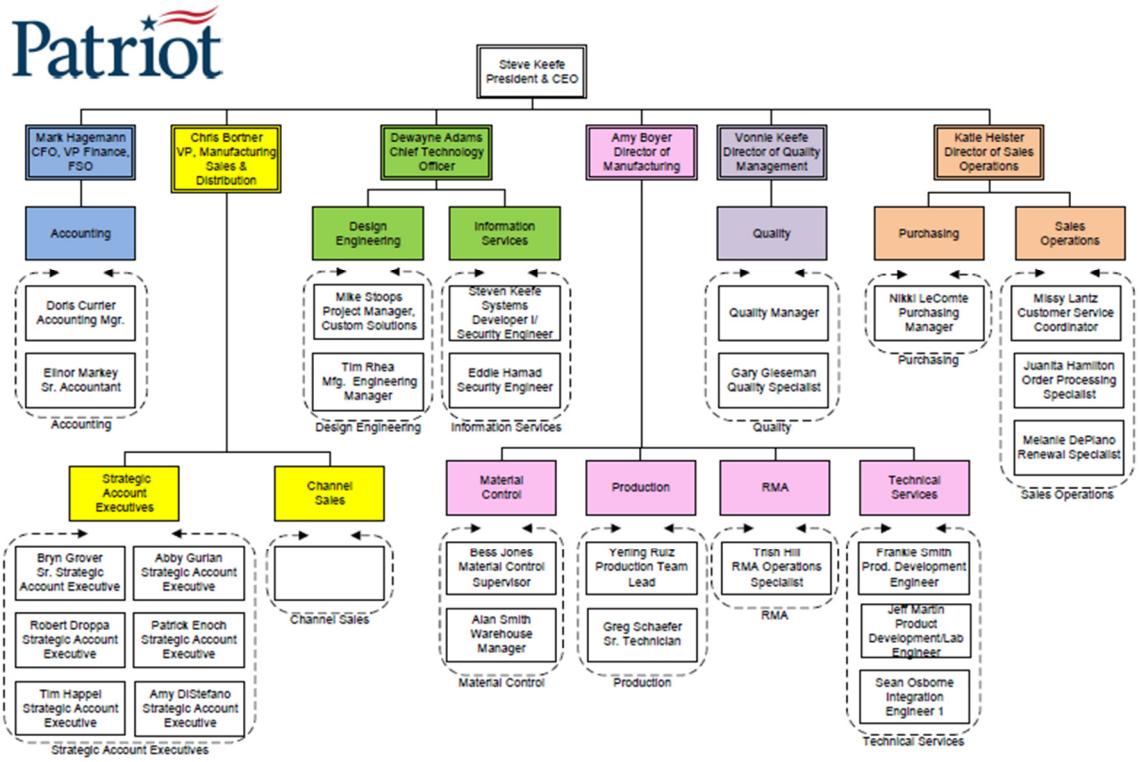
Patriot's team also bring extensive expertise to the project. Coming from various backgrounds in technology design and delivery, this team is prepared to deliver complex fully integrated solutions for a growing marketplace.

Steve Keefe, President & CEO - 30+ years of management and technical experience in the software development and manufacturing sectors. Previously spent 8 years working on projects with NSA with emphasis on real time operating systems and data acquisition. Spent over 10 years working on a variety of technical engineering activities related to hardware, software, firmware and applications in use by large and small companies. BS in Business Management from Radford University and currently holds a Top Secret security clearance

Dewayne Adams, CTO - Responsible for engineering, integration design, information technology and marketing. Extensive experience in solution development and successful deployment. Created first zero client laptop, first switchable NIAP-certified multi-domain remote desktop, advances in wearable computers and three patents covering these innovations along with others at NYNEX Science & Technology, Xybernaut and NCS Technologies. Studied Electrical Engineering & Mathematics - Tennessee Tech University & Stanford University. Holds a Top Secret security clearance

Mark Hagemann, CFO - 35+ years of international and domestic financial and business experience. Prior to join Patriot, Mark worked as VP of Finance and Operations at Innovative Therapies, VP Director of Financial Reporting at Interpublic Group of Companies and Director of FP&A at Cambrex. BS in Accounting from Villanova University, Maryland CPA certified. Holds a Top Secret security clearance

Michael Stoops, Project Manager, Custom Solutions - 20 years of Project Development and Management history including major projects for the USA DOD. 20 years of Project Budget Management, 25 years of Manufacturing and Engineering Process Development. 20 years Supply Chain Management. 15 years FCC and Safety Agency Certification Engineer. Four years FMF Program Management.



<u>Position to be filled by new employees:</u>
Electrical Engineer - Lead
Electrical Engineer
Mechanical Engineer - Lead
Mechanical Engineer
Industrial Designer - Lead
Industrial Designer
CAD Designer
Layout Engineer
Manufacturing Engineer
Certification

<u>Consultants and Subcontractors:</u>
Industrial Design Services
Certification Services

K. The Companies and Their Resources

K1. KAZUAR

KAZUAR Advanced Technologies Ltd. was founded in 2014 and is a privately held company. Its core business is developing innovative solutions in the cyber-security realm to premium customers who require the highest level of security. In its essence, the company presented a holistic approach to security, that is different than any other existing one. The company's success in developing the operational products is based on its team's extensive experience in intelligence, cyber-security and strategy.

KAZUAR's flagship solution is a secure PC environment that allows access to a secure system, protected against the highest level of threats. The company has launched the product, exceeded the original sales predictions and has gained acclaim for the prevention of significant attacks on its customers' systems. Among others, the company received a letter of appreciation from Colonel (Res.) Yohai Bar-Zakai, of the Rayzone group, stating the crucial role of the KAZUAR system in the defense of a customer, and the end result - prevention of any sensitive data leakage. The letter is attached to this application.

Following the success of the existing products, the company is in the last steps of raising significant funds from high-profile investors in the financial system. The funds are expected to be available to the company before the beginning of this program. These funds will both serve to expand the sales and marketing of the first product, as well as start the development of the products presented in this program.

The company is headquartered in Tel-Aviv offices, and includes a team of 8 dedicated employees, mostly with background and expertise in software, security, intelligence and operations. The company will use said funds to expand, and will approximately double its manpower and augment the development and marketing capabilities through a team of expert consultants. The current facilities already fit the extended personnel, and the full program presented to BIRD.

The company was chosen among 10 Israeli firms to participate in Intel's Ingenuity Partner Program, intended to propel success in promising startups in transformative fields, and hence receives additional support through this platform.

The company has yet to receive any funding in previous BIRD programs or from any state-funded project such as the OCS.

K2. Patriot

Headquartered in Chicago, IL, Patriot is a privately owned company by partners Steve Keefe. Patriot was founded in 1996 and has 21 years of experience in co-operation with security vendors, providing customized hardware and software to the Federal and State government. Patriot designs and delivers end-to-end customer solution of a similar nature to the one that will be designed in this project. Patriot's current facility of 35,000 square feet can accommodate the project with no additional labor additions. Certain network infrastructure, software and test equipment is required as outlined in the budget proposal. Additional expert-level sub-contractors and consultants for specific tasks are available from previous projects that the company did. The current structure and facility of the company can accommodate the project. Several tools need to be purchased as defined in the project budget.

Patriot maintains an employee headcount of approximately 70 based out of our Frederick Maryland facility. Several additional employees are based out of Texas, US. Patriot's work force is very stable with only a 4-5% annual turnover rate. This is primarily due to seasonal employees in our manufacturing and logistic division.
Patriot's corporate headquarters offers 20K square feet in manufacturing space, 2K square feet of R&D development area, 2K square feet of security development and training lab and a Security Operations Center for remote managed services. Warehouse space is approximately 10K square feet.
Patriot's annual revenue:
2016: 38,000K$
2017: Forecast is 42,000K$

Patriot participated in a previous BIRD grant for the development of a SCADA security infrastructure device. That project provided a unique Secure Smart-Grid Distributed Automation communication solution with integrated cyber security measures for the interaction between the Smart-Grid control center and the remote distributed automation devices. Such a secure platform will enable the reliable and secure monitoring and control of the distributed smart-grid assets.

The proposed solution was developed jointly by system engineers of Patriot and system architects of the Israeli Company. This co-operation leveraged the experience of both companies in the Smart-Grid and Security markets.

L. Project Budget

L1. KAZUAR Budget

ANNEX A

PROPOSED PROJECT BUDGET

Company name: KAZUAR
Project duration: 24 months

	Description	Details				Cost ($)	Total ($)
	I. Direct Labor						
	Employee's Name (TBD if yet unknown)	Employee's Profession	Employee location	Gross Annual Salary* ($)	% on Project	Cost to Project ($)	
Empl. 1:	Yuval Porat	CEO	IS	100,000	15%	30,888	
Empl. 2:	Moshe Azar	CTO	IS	100,000	53%	105,567	
Empl. 3:	Vered Dassa Levy	COO	IS	85,000	13%	21,658	
Empl. 4:	TBD	VP R&D	IS	100,000	89%	178,997	
Empl. 5:	Erez Gal Betzer	Senior Developer - client side	IS	100,000	51%	101,951	
Empl. 6:	TBD	Senior Developer - server side	IS	100,000	74%	147,945	
Empl. 7:	TBD	QA	IS	70,000	86%	120,189	
Empl. 8:	Naftali Rosenbaom	Hacker	IS	100,000	94%	187,455	
Empl. 9:	TBD	System Architect	IS	100,000	53%	105,312	
Empl.10:	Ran Kedar	IT Manager	IS	85,000	31%	52,048	
Empl. 11:	TBD	UI / UX Designer	IS	90,000	50%	90,616	
Empl. 12:	TBD	Firmware expert	IS	100,000	30%	59,178	
Empl. 13:					0%	0	
Empl. 14:					0%	0	
Empl. 15:					0%	0	
Empl. 16:					0%	0	
Empl. 17:					0%	0	
Empl. 18:					0%	0	
Empl. 19:					0%	0	
Empl. 20:					0%	0	
Empl. 21:					0%	0	
Empl. 22:					0%	0	
Empl. 23:					0%	0	
Empl. 24:					0%	0	
Empl. 25:					0%	0	
Empl. 26:					0%	0	
Empl. 27:					0%	0	
Empl. 28:					0%	0	
Empl. 29:					0%	0	
	Total, Direct Labor		* Including social benefits			1,201,804	
	Overhead @ 25%					300,451	
	Subtotal, Direct Labor + Overhead						1,502,255

	II. Equipment						
	Purchased Equipment Description	Purchased Cost ($/unit)	No. of Units	% On Project	% Annual Depreciation	Depre-ciation ($)	
Item 1	Computers	4,000	9	74%	33.3%	17,753	
Item 2				0%	33.3%	0	
Item 3				0%	33.3%	0	
Item 4				0%	33.3%	0	
Item 5				0%	33.3%	0	
Item 6				0%	33.3%	0	
Item 7				0%	33.3%	0	
Item 8				0%	33.3%	0	
Item 9				0%	33.3%	0	
Item 10				0%	33.3%	0	
Item 11				0%	33.3%	0	
Item 12				0%	33.3%	0	
Item 13				0%	33.3%	0	
Item 14				0%	33.3%	0	
Item 15				0%	33.3%	0	
	Subtotal, Purchased Equipment					17,753	

	Leased Equipment Description	Monthly Lease Cost ($/unit)	No. of Units	% On Project	Total Leasing Cost ($)	
Item 1				0%	0	
Item 2				0%	0	
Item 3				0%	0	
	Subtotal, Leased Equipment				0	
	Subtotal, Purchased or Leased Equipment					17,753

PROPOSED PROJECT BUDGET (cont.)

Company name: KAZUAR

	Description	Details	Cost ($)	Total ($)

III. Expendable Materials & Supplies

	Description	Cost ($)
Item 1		0
Item 2		0
Item 3		0
Item 4		0
Item 5		0
Item 6		0
Item 7		0
Item 8		0
Item 9		0
Item 10		0
Item 11		0
Item 12		0
Item 13		0
Item 14		0
Item 15		0
	Subtotal, Expendable Materials & Supplies	0

IV. Travel

Foreign Travel

	Destination	Purpose	Cost Per Person Per Trip ($)	No. of Trips	No. of People Per Trip	Duration Per Trip (days)	Cost ($)
Dest. 1	US	Pocket PC	7,500	2	1	7	15,000
Dest. 2	US	Display	7,500	1	1	7	7,500
Dest. 3	US	Keyboard	7,500	1	1	7	7,500
Dest. 4				0			0
Dest. 5				0			0
Dest. 6				0			0
Dest. 7				0			0
Dest. 8				0			0
Dest. 9				0			0
Dest. 10				0			0
Dest. 11				0			0
	Subtotal, Foreign Travel			4			30,000

Domestic Travel

	Destination	Purpose	Cost Per Person Per Trip ($)	No. of Trips	No. of People Per Trip	Duration Per Trip (days)	Cost ($)
Dest. 1				0			0
Dest. 2				0			0
Dest. 3				0			0
	Subtotal, Domestic Travel			0			0
	Subtotal, Travel						30,000

V. Subcontracts

	Service to be Performed	Name of Subcontractor	Country Service Given	Cost ($)
Subcont. 1	Pen testing	Deloitte / Hyver Security or other	IS	100,000
Subcont. 2	Global Certifications	Standards Institution of Israel or other	IS	10,000
Subcont. 3	Patent and IP consulting	Yigal Arnon & Co or other	IS	26,000
Subcont. 4	FIPS Consulting and US Certifications	Acuman or Penumbra Security or other	US	20,000
Subcont. 5	Industrial Design	TBD	IS	45,000
Subcont. 6	CTX tests	TBD	IS	4,000
	Subtotal, Subcontracts			205,000

VI. Consultants

	Service to be Performed	Name of Consultant & Country Service Given	Hourly Rate ($/Hr.)	No. of Hours	Cost ($)
Consult. 1	Senior Architect	Shimon Erlichman	150	112	16,800
Consult. 2	Senior Architect	Dr. Harel Menashrei	150	132	19,800
Consult. 3	Security Expert	TBD	150	120	18,000
Consult. 4	Cloud Security Expert	Itamar Kunik	150	80	12,000
Consult. 5	Physical Tampering Expert	Be'eri Katznelson	150	140	21,000
Consult. 6	Security Expert	Shlomi Marco	150	510	76,500
Consult. 7	Cryptografic consulting review	TBD	250	180	45,000
	Subtotal, Consultants				209,100

PROPOSED PROJECT BUDGET (cont.)

Company name:

Description	Details	Cost ($)	Total ($)
VII. Other Expenses			
		Cost ($)	
Item 1		0	
Item 2		0	
Item 3		0	
Item 4		0	
Item 5		0	
	Subtotal, Other Expenses		0
	Subtotal budget, before G&A Expenses		1,964,109
	General & Administrative Expenses (G&A) @5%		98,205
	Total Project Budget for Company		2,062,314

Projected Expenditure, by Segment	Segment Duration (months)	% of Total Budget	Projected Expenditure ($)
First segment			0
Second segment			0
Third segment			0
Fourth segment			0
Fifth segment			0
Sixth segment			0
Seventh segment			0
Eighth segment			0
Total	0	0%	0

L2. Patriot Budget

ANNEX A

PROPOSED PROJECT BUDGET

Company name: Patriot Technologies, Inc.
Project duration: 24 months

Description	Details	Cost ($)	Total ($)
I. Direct Labor			

	Employee's Name (TBD if yet unknown)	Employee's Profession	Employee location	Gross Annual Salary* ($)	% on Project	Cost to Project ($)
Empl. 1:	Dewayne Adams	Program Manager	US	150,000	6%	17,507
Empl. 2:	Mike Stoops	Project Manager	US	150,000	14%	41,178
Empl. 3:	Tim Rhea	Product Manager	US	135,000	14%	38,225
Empl. 4:	TBD	Electrical Engineer - Lead	US	115,000	13%	30,058
Empl. 5:	TBD	Electrical Engineer	US	85,000	20%	34,687
Empl. 6:	TBD	Mechanical Engineer - Lead	US	115,000	12%	28,214
Empl. 7:	TBD	Mechanical Engineer	US	85,000	26%	43,664
Empl. 8:	TBD	Industrial Designer - Lead	US	150,000	5%	15,411
Empl. 9:	TBD	Industrial Designer	US	85,000	7%	12,575
Empl.10:	TBD	CAD Designer	US	75,000	13%	19,849
Empl. 11:	TBD	Layout Engineer	US	75,000	11%	17,075
Empl. 12:	Jeff Martin	Test Engineer - Software	US	70,000	12%	16,627
Empl. 13:	Frankie Smith	Test Engineer - Hardware	US	70,000	19%	27,099
Empl. 14:	TBD	Manufacturing Engineer	US	75,000	14%	21,514
Empl. 15:	Sean Osborne	Integration Engineer	US	70,000	19%	26,351
Empl. 16:	TBD	Certification Engineer	US	65,000	29%	37,918
Empl. 17:					0%	0
Empl. 18:					0%	0
Empl. 19:					0%	0
Empl. 20:					0%	0
Empl. 21:					0%	0
Empl. 22:					0%	0
Empl. 23:					0%	0
Empl. 24:					0%	0
Empl. 25:					0%	0
Empl. 26:					0%	0
Empl. 27:					0%	0
Empl. 28:					0%	0
Empl. 29:					0%	0
Empl. 30:					0%	0
	Total, Direct Labor		* Including social benefits			427,953
	Overhead @ 25%					106,988
	Subtotal, Direct Labor + Overhead					534,941

II. Equipment

	Purchased Equipment Description	Purchased Cost ($/unit)	No. of Units	% On Project	% Annual Depreciation	Depre-ciation ($)
Item 1	Tooling for MSC	150,000	1	45%	33.3%	45,205
Item 2	Tooling for SD	150,000	1	33%	33.3%	32,877
Item 3	Tooling for SID	200,000	1	33%	33.3%	43,836
Item 4				0%	33.3%	0
Item 5				0%	33.3%	0
Item 6				0%	33.3%	0
Item 7				0%	33.3%	0
Item 8				0%	33.3%	0
Item 9				0%	33.3%	0
Item 10				0%	33.3%	0
Item 11				0%	33.3%	0
Item 12				0%	33.3%	0
Item 13				0%	33.3%	0
Item 14				0%	33.3%	0
Item 15				0%	33.3%	0
	Subtotal, Purchased Equipment					121,918

	Leased Equipment Description	Monthly Lease Cost ($/unit)	No. of Units	% On Project	Total Leasing Cost ($)	
Item 1				0%	0	
Item 2				0%	0	
Item 3				0%	0	
	Subtotal, Leased Equipment				0	
	Subtotal, Purchased or Leased Equipment					121,918

PROPOSED PROJECT BUDGET (cont.)

Company name: Patriot Technologies, Inc.

	Description	Details	Cost ($)	Total ($)

III. Expendable Materials & Supplies

	Description	Cost ($)
Item 1	Samples of MSC for Test	25,000
Item 2	Samples of SD for Test	21,000
Item 3	Samples of SID for Test	25,000
Item 4		0
Item 5		0
Item 6		0
Item 7		0
Item 8		0
Item 9		0
Item 10		0
Item 11		0
Item 12		0
Item 13		0
Item 14		0
Item 15		0
	Subtotal, Expendable Materials & Supplies	71,000

IV. Travel

Foreign Travel

	Destination	Purpose	Cost Per Person Per Trip ($)	No. of Trips	No. of People Per Trip	Duration Per Trip (days)	Cost ($)
Dest. 1	Israel	Project Meeting	3,000	3	1	5	9,000
Dest. 2	Taiwan	Inprocess Verification	3,500	1	2	5	7,000
Dest. 3				0			0
Dest. 4				0			0
Dest. 5				0			0
Dest. 6				0			0
Dest. 7				0			0
Dest. 8				0			0
Dest. 9				0			0
Dest. 10				0			0
Dest. 11				0			0
	Subtotal, Foreign Travel			4			16,000

Domestic Travel

	Destination	Purpose	Cost Per Person Per Trip ($)	No. of Trips	No. of People Per Trip	Duration Per Trip (days)	Cost ($)	
Dest. 1	San Jose, CA	PCB Review	2,000	2	2	4	8,000	
Dest. 2	Denver, CO	Manufacturing Review	2,000	1	1	4	2,000	
Dest. 3	San Francisco, CA	Industrial Design	2,500	4	2	4	20,000	
		Subtotal, Domestic Travel		7			30,000	
		Subtotal, Travel						46,000

V. Subcontracts

	Service to be Performed	Name of Subcontractor		Country Service Given	Cost ($)	
Subcont. 1	Industrial Design Services	New Deal Design		US	120,000	
Subcont. 2	Certification Services	MetLabs		US	45,000	
Subcont. 3					0	
Subcont. 4					0	
Subcont. 5					0	
Subcont. 6					0	
	Subtotal, Subcontracts					165,000

VI. Consultants

	Service to be Performed	Name of Consultant & Country Service Given	Hourly Rate ($/Hr.)	No. of Hours	Cost ($)	
Consult. 1				0	0	
Consult. 2				0	0	
Consult. 3				0	0	
Consult. 4				0	0	
Consult. 5				0	0	
Consult. 6				0	0	
	Subtotal, Consultants					0

PROPOSED PROJECT BUDGET (cont.)

Company name:

	Description	Details	Cost ($)	Total ($)
	VII. Other Expenses			
			Cost ($)	
Item 1			0	
Item 2			0	
Item 3			0	
Item 4			0	
Item 5			0	
	Subtotal, Other Expenses			0
	Subtotal budget, before G&A Expenses			938,859
	General & Administrative Expenses (G&A) @5%			46,943
	Total Project Budget for Company			985,802

Projected Expenditure, by Segment

	Segment Duration (months)	% of Total Budget	Projected Expen-diture ($)
First segment			0
Second segment			0
Third segment			0
Fourth segment			0
Fifth segment			0
Sixth segment			0
Seventh segment			0
Eighth segment			0
Total	0	0%	0

M. Risk Analysis

TABLE 1A

			Impact		
Risk #	Name/Description	Ranking	Duration[1]	Budget[2]	Commercialization Potential[3]
1	Delay in Development	Medium	Medium	Medium	Low
2	Sales lower than expectations	Low	Low	Low	Medium
3	Crowded Competition	Very Low	Low	Medium	Medium
4	Descent in Cyber Security Market	Very Low	Low	Low	Medium
5	Lack of collaboration between the Israeli and American Teams	Very Low	Low	Low	Low

TABLE 1B

Risk #	Name/Description	Type*
1	Delay in Development due to technical issues or collaboration failures between teams that leads to delayed delivery	(T)
2	Sales lower than expectations due to new sales process in different markets, learning curve slower than expected	(M)
3	Crowded Competition of similar solutions both for mobile or PC environments or other applications with similar offering	(E)
4	Descent in Cyber Security Market both on investments side and immediate need due to external circumstances	(E)
5	Lack of collaboration between the Israeli and American Teams that might affect project's progress	(M)

*Type: Technical (T), Project Management/Resources (M), External to the Project (E)

N. Sundry Information

To enable the Foundation to prepare CPFA, on timely basis following approval of the grant application by BIRD's Board of Governors, please provide the following information in the proposal:

Venue for the applicable law governing the CPFA between the companies and the Foundation: Israel.

N1. KAZUAR Details

- Project manager

Name	Direct phone number	e-mail address	Position
Yuval Porat	972-50-7799000	yuval@kazuar-tech.com	CEO

- Fiscal Information Official

Name	Direct phone number	e-mail address
Tal Sharon	972-52-6702967	tal@kazuar-tech.com

- Bank account details

Account name	Account number	Bank name	Branch number
KAZUAR Advanced Technologies Ltd.	331254	Hapoalim	558
Bank address			
132 Menachem Begin Rd., 67021 Tel Aviv			
IBAN number			
IL08-0125-5800-0000-0331-254			

N2. Patriot Details

- Project manager

Name	Direct phone number	e-mail address	Position
Mike Stoops	+1-301-695-7500	mstoops@patriot-tech.com	Project Manager, Custom Solutions

- Fiscal Information Official

Name	Direct phone number	e-mail address
Mark Hagemann	301-695-7500	mhagemann@patriot-tech.com

- Bank account details

Account name	Account number	Bank name	Branch number
Patriot Technologies	4294333299	Wells Fargo	410-332-5525
Bank address			
7 Saint Paul Street, Baltimore, MD 21202			
Routing number			
ABA 121000248 SWIFT CODE WFB1US6S			

Appendix A - Certificates of Incorporation

KAZUAR

מדינת ישראל
משרד המשפטים – רשות התאגידים
רשם החברות והשותפויות

תעודת התאגדות חברה

וזאת לתעודה כי החברה :

קזואר טכנולוגיות מתקדמות בע"מ

KAZUAR ADVANCED TECHNOLOGY LTD

שמספרה 515081529

נתאגדה ונרשמה ביום 19/05/2014 י"ט אייר תשע"ד
על פי חוק החברות, התשנ"ט-1999, כחברה בערבון מוגבל.

ניתנה בירושלים ביום:

19/05/2014
י"ט אייר תשע"ד

משרד המשפטים
רשם החברות והשותפויות

אביבה ברוך, עו"ד
רשות התאגידים
רשם החברות והשותפויות

Patriot

ARTICLES OF INCORPORATION
OF
PATRIOT TECHNOLOGIES, INC.

APPROVED AND RECEIVED FOR RECORD BY THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION OF MARYLAND JANUARY 23, 1996 AT 11:40 O'CLOCK A. M. AS IN CONFORMITY WITH LAW AND ORDERED RECORDED.

ORGANIZATION AND CAPITALIZATION FEE PAID:	RECORDING FEE PAID:	SPECIAL FEE PAID:
$ 20.00	$ 20.00	$

D4313359

IT IS HEREBY CERTIFIED, THAT THE WITHIN INSTRUMENT, TOGETHER WITH ALL INDORSEMENTS THEREON, HAS BEEN RECEIVED, APPROVED AND RECORDED BY THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION OF MARYLAND.

WEST & FEINBERG, P.C.
4550 MONTGOMERY AVENUE
SUITE 775N
BETHESDA MD 20814

153271

1-23-96 1140a

ARTICLES OF INCORPORATION

OF

PATRIOT TECHNOLOGIES, INC.

FIRST: The undersigned, Marc R. Feinberg, whose post office address is 4550 Montgomery Avenue, Suite 775N, Bethesda, Maryland 20814, being over eighteen years of age and acting as incorporator, hereby forms a corporation under the general laws of the State of Maryland.

SECOND: The name of the corporation (which is hereinafter called the "Corporation") is:

PATRIOT TECHNOLOGIES, INC.

THIRD: The purposes for which the Corporation is formed are as follows:

(a) To engage in the sale and resale of high tech computer hardware, software and services; and

(b) To engage in any other lawful business.

FOURTH: The post office address of the principal office of the Corporation in the State of Maryland is 906 Autumn Ridge Court, Mount Airy, Maryland 21771. The resident agent of the Corporation is Bruce F. Tucker, whose post office address is 906 Autumn Ridge Court, Mount Airy, Maryland 21771. Said resident agent is an individual, who is a citizen of and resides in the State of Maryland.

FIFTH: The Corporation shall have three (3) directors (which number may be increased or decreased pursuant to the Bylaws of the Corporation). The initial directors of the Corporation shall be Bruce F. Tucker, Scott F. Tucker and Saul S. Levine, who shall serve in such capacity until the first annual meeting of the

60258257

3784 1233

stockholders, or until their successors are duly elected and qualified.

SIXTH: The total number of shares of capital stock which the Corporation has authority to issue is Two Hundred Thousand (200,000), divided into 100,000 shares of Class A Common Stock par value ten cents ($.10) and 100,000 shares of Class B Common Stock par value ten cents ($.10).

The following is a description of each class of stock of the Corporation with the preferences, conversion and other rights, restrictions, voting powers, and qualifications of each class:

1. Except as hereinafter provided with respect to voting powers, the Class A Common Stock and the Class B Common Stock of the Corporation shall be identical in all respects.

2. With respect to voting powers, except as otherwise required by the Corporations and Associations Article of the Annotated Code of Maryland, the holders of Class A Common Stock shall possess all voting powers for all purposes including, by way of illustration and not of limitation, the election of directors, and the holders of Class B Common Stock shall have no voting power whatsoever, and no holder of Class B Common Stock shall vote on or otherwise participate in any proceedings in which actions shall be taken by the Corporation or the stockholders thereof or be entitled to notification as to any meeting of the Board of Directors or the stockholders.

SEVENTH: The following provisions are hereby adopted for the purpose of defining, limiting and regulating the powers of the Corporation and of the directors and stockholders:

(a) The Board of Directors of the Corporation is empowered to authorize the issuance from time to time of shares of its stock of any class, whether now or hereafter authorized, and securities convertible into shares of its stock, of any class or classes, whether now or hereafter authorized, for such consideration as the Board of Directors may deem advisable.

(b) The Corporation reserves the right to make, from time to time, any amendments of its charter which may now or hereafter be authorized by law, including any amendments which alter the contract rights of any class of outstanding stock as expressly set forth in the charter.

(c) The Board of Directors shall have the power to classify or reclassify any unissued stock, whether now or hereafter authorized, by setting or changing the preferences, conversion or other rights, voting powers, restrictions, limitations as to dividends, qualifications, or terms or conditions of redemption of such stock.

IN WITNESS WHEREOF, I have signed these Articles of Incorporation on the 23rd day of January, 1996, and have acknowledged such Articles to be my act.

Witness

Marc R. Feinberg
Incorporator

\15327\ART.INC

142C3097118

A 510668

RECORDED IN THE RECORDS OF THE

STATE DEPARTMENT OF ASSESSMENTS

AND TAXATION OF MARYLAND IN LIBER. FOLIO.

5-083

Appendix B – Rayzone's appreciation

Rayzone Group

13/10/2016

To
Yuval Porat
CEO
KAZUAR Advanced Technologies Ltd

Re: **KAZUAR**

Dear Yuval,

I would like to personally thank you for successfully taking care of a major crisis regarding a very important customer of ours, who deals with top secret information.

As you know, at the end of the past week the customer discovered that one of his employees committed a very severe violation of security protocols and didn't even care to report it.

Based on my extensive experience in the intelligence community, I can testify that usually even a less severe security violation would lead to a significant data leak, and in this specific case - even a partial data leak would have led to profoundly negative consequences.

In this rare case - due to our decision to provide the customer with KAZUAR Secured Working Environment, there has been no data leak at all. I am confident that no other solution would have been able to deal with such an extreme security violation. The customer and I believe that this crisis management supports beyond any doubt our choice to use KAZUAR and proves that this is the perfect solution for every organization that deals with sensitive information.

In addition, I would like to thank KAZUAR's team for the immediate and professional response, which allowed the customer to rapidly receive a report of the situation and also obtain alternative equipment very quickly.

You are more than welcome to share this letter.

Thank you very much and best regards,

Yohai Bar Zakai
Colonel (Res.)
Rayzone Group

- Cutting edge solutions for innovative intelligence –
Rayzone Group Ltd. 65 Yigal Alon St. Toyota House, Tel Aviv, Israel, 67443.
Tel: +972-73-2802266 ; Fax:+ 972-73-2802260; info@rayzoneg.com ; www.rayzoneg.com